UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

SIMO HOLDINGS INC., SKYROAM, INC., AND SHENZHEN SKYROAM TECHNOLOGY CO., LTD.,

Plaintiffs

v.

HONG KONG UCLOUDLINK NETWORK TECHNOLOGY LIMITED, SHENZHEN UCLOUDLINK NETWORK TECHNOLOGY CO. LTD., AND SHENZHEN UCLOUDLINK NEW TECHNOLOGY CO. LTD,

Defendants.

CIVIL ACTION NO. _____

JURY TRIAL DEMANDED

[redacted]

COMPLAINT

Plaintiffs SIMO Holdings Inc. ("SIMO"), Skyroam, Inc., and Shenzhen Skyroam Technology Co., Ltd. ("Skyroam Shenzhen") (Skyroam, Inc. and Skyroam Shenzhen are referred to hereinafter as "Skyroam"; SIMO and Skyroam are referred to collectively hereinafter as "Plaintiffs"), by and through counsel of record, assert the following claims of patent infringement and misappropriation of trade secrets against Defendants Hong Kong uCloudlink Network Technology Limited ("uCloudlink Hong Kong"); Shenzhen uCloudlink Network Technology Co. Ltd. ("uCloudlink Shenzhen"); and Shenzhen uCloudlink New Technology Co. Ltd. ("uCloudlink New") (referred to collectively hereinafter as "Defendants").

SUMMARY OF THE ACTION

1. This is an action for infringement of United States Patent No. 9,736,689 entitled "System and Method for Mobile Telephone Roaming" ("the '689 Patent") by uCloudlink's WiFi hotspot devices and mobile phones that do not fall within the scope of a permanent injunction previously ordered by the Southern District of New York.

2. This is also an action for misappropriation of trade secrets associated with Defendants making, using, selling, and offering for sale the same devices.

THE PARTIES

3. SIMO Holdings Inc. is a company incorporated under the laws of Cayman Islands with a principal place of business at Xihai Mingzhu Building, 1001 Nanshan District, Taoyuan Road Shenzhen City, Guangdong Province, People's Republic of China.

4. Skyroam, Inc. is a company incorporated under the laws of the state of California with a principle place of business at 180 Sansome Street, Suite 200, San Francisco, CA 94104.

5. Skyroam Shenzhen is a company incorporated under the laws of the People's Republic of China with a principal place of business at Block F, 710-716 Xihai Mingzhu Building, Taoyun Road, Nanshan District Shenzhen, 518052, People's Republic of China.

6. Upon information and belief, Defendant Hong Kong uCloudlink Network Technology Limited is a company incorporated under the laws of Hong Kong SAR, China, with a principal place of business at 29/F, One Pacific Centre, 414 Kwun Tong Road, Kwun Tong, KLN, Hong Kong, SAR China.

7. Upon information and belief, Defendant Shenzhen uCloudlink Network Technology Co. Ltd. is a company incorporated under the laws of the People's Republic of China with a registered address at 301-306, Block A, Building 1, Shenzhen Software Industry Base, Xuefu Road, Yuehai Neighborhood, Nanshan District, Shenzhen, People's Republic of China.

8. Upon Information and Belief, Defendant Shenzhen uCloudlink New Technology Co. Ltd. is a company incorporated under the laws of the People's Republic of China with a registered address at 301-306, Block A, Building 1, Shenzhen Software Industry Base, Xuefu Road, Yuehai Neighborhood, Nanshan District, Shenzhen, People's Republic of China.[1]

OTHER RELEVANT ENTITIES

9. Upon information and belief, Ucloudlink (America), Ltd. is a company incorporated under the laws of the state of New York, with a principal place of business at 205 East 42nd Street, 20th Floor, New York, NY 10017.

10. Upon information and belief, uCloudlink (HK) Limited ("uCloudlink HK") is a company incorporated under the laws of Hong Kong SAR, China, with a registered address at Suite 603, 6/F, Laws Commercial Plaza, 788 Cheung Sha Wan Road, Kowloon, Hong Kong, SAR China.

11. Upon information and belief, uCloudlink Group, Inc. ("uCloudlink Cayman") is a company incorporated under the laws of the Cayman Islands, with a registered address at P.O. Box 2075, # 31 The Strand, 46 Canal Point Drive, Grand Cayman KY1-1105, Cayman Islands.

12. Upon information and belief, uCloudlink Hong Kong, uCloudlink (HK) and uCloudlink Shenzhen, are wholly owned subsidiaries (either directly or indirectly) of uCloudlink Cayman.

13. Upon information and belief, by virtue of a change in the corporate structure, uCloudlink Hong Kong now has 100% control over uCloudlink New, either by virtue of uCloudlink Hong Kong's ownership of uCloudlink HK, by virtue of a change in corporate control,

[1] uCloudlink Hong Kong and uCloudlink Shenzhen are referred to herein as the "Misappropriation Defendants." The totality of the uCloudlink entities, with the exception of uCloudlink Cayman, are referred to herein as the "uCloudlink Group."

or through the treatment of uCloudlink New as part of the greater uCloudlink enterprise that completely disregards corporate formalities and treats all uCloudlink entities as part of one entity, as explained below.

14. Upon information and belief, until approximately May 16, 2019, uCloudlink HK was the parent company of uCloudlink Hong Kong, uCloudlink Shenzhen, and had a 100% controlling interest in uCloudlink New.

15. Upon information and belief, on or about May 16, 2019, uCloudlink HK transferred its ownership shares in uCloudlink Hong Kong to uCloudlink Cayman.

16. As a result, upon information and belief, beginning on or about May 16, 2019, uCloudlink Hong Kong, operating as a subsidiary of uCloudlink Cayman, wholly owns uCloudlink HK and uCloudlink Shenzhen, and has a 100% controlling interest in uCloudlink New.

17. The entities making up the uCloudlink Group operate, act, represent, and market themselves as a single entity.

18. uCloudlink's promotional materials refer to the entities making up the uCloudlink Group as a single entity with different "branches," and employees of the respective uCloudlink entities refer to uCloudlink as a single "uCloudlink" company.

19. As another example, the uCloudlink "[redacted]

[redacted]

20. By virtue of the uCloudlink Group's organizational structure and functional relationships, its members should be treated as a single entity, or at a minimum, should not be permitted to hide behind the protections afforded to purportedly different corporate entities.

21. Upon information and belief, DHI Group Limited, LLC, F/K/A DHI Telecom Group, is a company incorporated under the laws of Texas with its principal place of business at 9251 Park South View, Houston, Texas, 77051.

22. DHI is an American telecommunications company that provides wireless hotspots and phones, and associated internet services to consumers in the United States and abroad. A significant part of the DHI business model involves providing these products and services to members of the United States armed forces through sales at military exchange stores in the United States and on bases outside the United States.

SKYROAM'S TECHNOLOGY AS THE FOUNDATION OF UCLOUDLINK'S BUSINESS MODEL

23. This case involves so-called virtual SIM technology. This virtual SIM technology enables the business model of both Plaintiffs and Defendants.

24. In particular, by virtue of this virtual SIM technology, users of Defendants' devices can travel internationally and use data without having to pay expensive roaming fees or purchase a country-specific SIM card for each new country visited.

25. The uCloudlink Group enables its customers to access data through the uCloudlink devices by housing physical SIM cards from various cellular network providers—including United States cellular network providers such as AT&T, T-Mobile, Cricket, and Verizon—in SIM banks located in the administrative systems (i.e., servers) centrally operated by [redacted]

[redacted]

26. An uCloudlink hotspot or phone device cannot use cellular data in, for example, Texas, without the receipt of the virtual or cloud SIM, which is always obtained from the servers operated by [redacted] and delivered over local (i.e., United States-based) cellular networks directly to devices in Texas via software developed by [redacted].

27. This operation and delivery [redacted] is a piece of the overall scheme by uCloudlink Group, and specifically by [redacted] New to provide working devices and services in the United States.

28. On information and belief, [redacted] tracks the delivery of virtual SIM devices and knows exactly where and when a virtual SIM is delivered in the United States.

29. By way of example, on information and belief, when [redacted] intends for a virtual SIM device to be delivered to a WiFi hotspot or mobile phone in Marshall, Texas, [redacted] tracks that delivery and has the ability to confirm its delivery to the WiFi hotspot or mobile phone in Marshall, Texas.

30. Employees nominally contracted to each entity in the uCloudlink Group play an integral role in the operation, development, marketing, manufacturing, sale, customer support, and rental services of the devices to business partners and consumers.

31. Each entity in the uCloudlink Group intends that the devices can and will be used in the United States.

32. The uCloudlink Group sells and rents its devices and services under several brand

names, including the "GlocalMe" and "RoamingMan" brands.

33. The uCloudlink Group develops, manufactures, supports, markets, provides data to, sells, and/or rents the uCloudlink devices and platform using this technology to consumers, business partners, and so-called "white label partners," who sell or rent the uCloudlink devices and services under their own brand.

34. The uCloudlink devices, whether branded as uCloudlink devices or branded separately by white label partners, only operate as a closed system via data packages developed, supported, sold, or otherwise enabled by uCloudlink. This means that a consumer cannot access the local cellular networks on an uCloudlink device through a virtual SIM provided by any other third party, such as Plaintiffs.

35. With regard to uCloudlink's white label partners, uCloudlink sells unbranded devices (such as WiFi hotspots) to third parties for sale under those third parties' brand names. uCloudlink also works with those partners to develop their own white-label branded software portal that links to uCloudlink's data services. DHI is one such white label partner.

36. DHI provides WiFi Hotspots and related services to its United States customers under its Sapphire and Tep Wireless and/or Travel WiFi brands using uCloudlink's Cloud SIM technology. The hardware, software, and backend data services used by DHI's products are developed, supported, designed, produced, and sold to DHI by uCloudlink Hong Kong, uCloudlink Shenzhen, and uCloudlink New.

37. DHI focuses its sales and marketing efforts with regard to rebranded uCloudlink devices in the United States and at United States military bases overseas.

38. DHI specifically markets its Sapphire-branded uCloudlink Cloud SIM devices to members of the United States Armed Forces and their families so that they may utilize internet

services and send information among each other while they are abroad in war zones and on military bases.

THE HISTORY OF THE PARTIES' DISPUTES

SIMO's New York Patent Action

1. SIMO Prevails on its Patent Infringement Claim

39. In June 2018, SIMO filed a patent infringement suit in the Southern District of New York against uCloudlink Hong Kong and uCloudlink America in civil case captioned *SIMO Holdings, Inc. v. Hong Kong uCloudlink Network Technology Limited and Ucloudlink (America) Limited*, Case No. 18-cv-5427 (JSR) (the "New York Patent Action").

40. In the New York Patent Action, SIMO alleged that uCloudlink Hong Kong and uCloudlink America infringed the '689 Patent.

41. The Southern District of New York granted summary judgment that uCloudlink's devices literally infringed the '689 Patent, and a jury found that uCloudlink willfully infringed the '689 Patent and that the '689 Patent was not invalid. The District Court issued a permanent injunction, which precluded uCloudlink from importing, selling, offering to sell, or enabling, the four infringing uCloudlink Devices at issue in the New York litigation (the "Infringing Devices").

42. uCloudlink Hong Kong and uCloudlink America thereafter sought modification of the injunction, contending that a software update it purportedly pushed out to the Infringing Devices rendered those devices (the "Redesigned Devices") more than colorably different from the Infringing Devices. SIMO disagreed.

43. Over SIMO's objection, the Southern District of New York modified the injunction and permitted uCloudlink to sell and enable data on the Redesigned Devices.[2]

[2] At the time of the filing of this Complaint, SIMO's motion for reconsideration of the Southern District of New York's modification of the permanent injunction remains pending.

44. The Southern District of New York has never ruled on whether the Redesigned Devices infringe the '689 Patent.

2. SIMO Discovers uCloudlink's Trade Secret Theft

45. During the New York Patent Action, uCloudlink Hong Kong and uCloudlink America produced hundreds of thousands of documents.

[redacted]

48. Several of the documents produced by uCloudlink Hong Kong and uCloudlink America in the New York Patent Action contain highly confidential technical trade secret information created and owned by Skyroam Shenzhen.[3] These documents include key technical information for Skyroam's first mobile hotspot device and backend systems.

49. Specifically, uCloudlink produced highly confidential Skyroam Shenzhen documents that it claimed to have obtained from its search of the uCloudlink work computer of then-uCloudlink Shenzhen employee Wang Bin (referred to hereinafter as "Mr. Wang").

50. Mr. Wang was at one point employed by Skyroam Shenzhen.

51. Mr. Wang left Skyroam Shenzhen for uCloudlink in 2013.

52. uCloudlink also produced certain confidential internal Skyroam and uCloudlink documents which refer specifically to, and in some instances quote word for word, confidential trade secret information belonging to Skyroam Shenzhen. Though similar to the documents uCloudlink claimed to have obtained from Mr. Wang's uCloudlink computer, Mr. Wang is not

[3] Those documents are referred to hereinafter as the "Skyroam Confidential Documents."

listed as the custodian of these documents. This demonstrates that the Skyroam confidential documents were utilized by uCloudlink employees other than Mr. Wang.

uCloudlink's California Patent Action

53. In August 2018, uCloudlink Hong Kong and uCloudlink America filed a patent infringement lawsuit in the Northern District of California against SIMO and Skyroam in a civil action captioned *Hong Kong uCloudlink Network Technology Limited and Ucloudlink (America) Limited v. SIMO Holdings, Inc. and Skyroam, Inc.*, Case No. 18-cv-05031 (EMC) (the "California Patent Action").

54. In the California Patent Action, uCloudlink Hong Kong and uCloudlink America allege that SIMO and Skyroam, Inc. infringe U.S. Patent No. 9,548,780 ("'780 Patent").

55. The '780 Patent was filed in 2013, months after Mr. Wang left Skyroam Shenzhen for uCloudlink Shenzhen's predecessor entity with Skyroam's confidential trade secrets in tow.

56. Based on the discovery in the New York Patent Action, Plaintiffs sought to bring a counterclaim in the California Patent Action for misappropriation of trade secrets against uCloudlink Hong Kong and uCloudlink America.

57. Plaintiffs first sought to amend their counterclaim to add trade secret claims against the existing plaintiffs in the California action (uCloudlink Hong Kong and uCloudlink America) and to add a new uCloudlink entity under the trade secret allegations (uCloudlink Shenzhen). The District Court for the Northern District of California allowed the addition of the trade secret claims, but denied the motion to add uCloudlink Shenzhen without prejudice and ordered jurisdictional discovery with respect to uCloudlink Shenzhen. During the jurisdictional discovery in the California Patent Action and review of documents produced during the then-ongoing New York Patent Action, Plaintiffs learned of the connections between the uCloudlink Group, and specifically uCloudlink Shenzhen, uCloudlink New, and DHI, which is a Texas based company.

The plaintiff uCloudlink entities in the California Patent Action (uCloudlink Hong Kong and uCloudlink America) subsequently moved to dismiss the trade secret claims based primarily on the argument that there were insufficient allegations of a conspiracy to commit trade secret misappropriation between Mr. Wang and those entities. Following uCloudlink Hong Kong and uCloudlink America's motion to dismiss under Federal Rule 12(b)(6), the District Court for the Northern District of California dismissed Plaintiffs' counterclaims with prejudice, finding there were—at that time and given the then-existing corporate structure of uCloudlink—insufficient allegations of a conspiracy between Mr. Wang and either uCloudlink Hong Kong or uCloudlink America to establish a conspiracy to commit trade secret misappropriation. California Patent Action at Dkt. 103.

58. The Northern District of California neither analyzed nor ruled upon Plaintiffs' allegations that uCloudlink Hong Kong and uCloudlink America could be held liable for misappropriation of trade secrets under alternative theories such as alter ego or *respondeat superior*.

59. The Northern District of California has never been presented with the evidence obtained through jurisdictional discovery related to whether personal jurisdiction is appropriate in Texas that forms the basis for jurisdiction in this action over uCloudlink Shenzhen.

uCloudlink's Recent Corporate Changes

60. The Defendants in the instant action are *different* than the parties against whom Plaintiffs previously sought to bring a claim of trade secret misappropriation in the California Patent Action.

61. The corporate structure of the uCloudlink entities has changed since Plaintiffs were engaged in motion practice before the California court with respect to their counterclaims for conspiracy to commit misappropriation of trade secrets against uCloudlink America and Hong

Kong.

62. In particular, uCloudlink Hong Kong has recently taken over sole ownership of the uCloudlink entities other than uCloudlink New and uCloudlink's Cayman Island-based holding company.

63. Upon information and belief, uCloudlink New, although owned by six individuals, and not a subsidiary of uCloudlink Cayman, [redacted].

64. Upon information and belief, by virtue of the change of the corporate structure, uCloudlink Hong Kong [redacted] New, either by virtue of uCloudlink Hong Kong's ownership of uCloudlink HK, by virtue of a change in corporate control, or through the uCloudlink Group's treatment of uCloudlink New as part of the greater uCloudlink enterprise that completely disregards corporate formalities and treats all uCloudlink entities as part of one entity as explained herein.

65. These corporate changes and additional information learned through discovery are the reason the named Defendants in the instant action are different than those against whom trade secret misappropriation was alleged in the Northern District of California.

66. Because of at least the changes in corporate structure, uCloudlink Hong Kong is now knowingly benefitting from misappropriated trade secrets that were first misappropriated by and then later disclosed in patent applications and subsequently used by uCloudlink Shenzhen.

The uCloudlink Group Has Consistently Failed to Observe Corporate Formalities Such that it Acts as a Single Business and Each uCloudlink Entity is an Alter Ego of the Other

67. Even before the shuffling of the uCloudlink Group's corporate structure, the uCloudlink Group did not and, to date, does not observe corporate formalities that would be expected of separate and distinct corporate entities. Indeed, the uCloudlink Group acts as a single business and each uCloudlink entity is an alter ego of the other.

68. Upon information and belief, the uCloudlink Group does not differentiate between the various uCloudlink entities that own or have access to its intellectual property, source code, business information, and documents. The uCloudlink Group intermingles the storage of such information in a single Shenzhen location, with a mirror in Hong Kong.

69. [redacted] In other words, the uCloudlink Group does not differentiate its employees by their "contracting entity" and instead differentiates them based on the type of work they perform or project group.

70. Upon information and belief, employees of the various entities within the uCloudlink Group are not bound by the corporate hierarchy of their respective contracting entity. Such employees are required to comply with instructions and directives of employees and executives employed by other uCloudlink entities based on the requirements of a given project.

71. Consistent with the fact that there is no meaningful distinction between the companies, an uCloudlink announcement from the [redacted]

[redacted]t. These appointments refer to the structure of the uCloudlink Group, as a singular corporate enterprise, and not to any specific uCloudlink entity.

[redacted].

73. The uCloudlink Group Head Office [redacted]

- [redacted]
- [redacted]
- [redacted]

74. The conduct of the uCloudlink entities during the New York Patent Case further supports the notion that the uCloudlink companies are alter egos of one another.

75. By way of example, uCloudlink Hong Kong and/or uCloudlink America produced Zhenhui Liu, an employee of [redacted] and not an employee of [redacted] for a deposition in the New York Patent Case. Zhenhui Liu testified not on behalf of u[redacted]—she testified in her personal capacity.

76. Likewise, uCloudlink Hong Kong and/or uCloudlink America produced Ailiang Zhou, an employee of [redacted] and not an employee of [redacted]—for a deposition in the New York Patent Case. Like Zhenhui Liu, Ailiang Zhou testified in his personal capacity, and not on behalf of [redacted]

77. uCloudlink Hong Kong and/or uCloudlink America produced Hongye Sun, an employee of [redacted] and not an employee of [redacted] for a deposition in the New York Patent Case. Like Zhenhui Liu and Ailiang Zhou, Hongye Sun testified in his personal capacity, and not on behalf of [redacted]

78. uCloudlink Hong Kong and/or uCloudlink America produced He Shu, an employee of [redacted] and not an employee of [redacted]—for a deposition in the New York Patent Case. Like Zhenhui Liu, Ailiang Zhou, and Hongye Sun, He Shu testified in his personal capacity and not on behalf of [redacted]

79. At the depositions of Zhenhui Liu, Aliang Zhou, Hongye Sun, and He Shu, Counsel

for uCloudlink Hong Kong and uCloudlink America represented only uCloudlink Hong Kong and uCloudlink America. Counsel for uCloudlink America and uCloudlink Hong Kong did not represent [redacted] at these depositions.

80. In the New York Patent Action, Zhenhui Liu, [redacted]. Counsel for uCloudlink Hong Kong and uCloudlink America designated this testimony as corporate testimony on behalf of uCloudlink Hong Kong and uCloudlink America.

81. uCloudlink Shenzhen has been directly involved in working with United States-based white label companies such as DHI Telecom, [redacted] to enable those companies to sell, implement, use, and/or otherwise access technology that utilizes SIMO's trade secrets.

82. uCloudlink Shenzhen manufactures products, designs product packaging and labeling, creates technical execution plans, provides technical solutions and trainings for the U.S. customers, mails products to U.S. customers, and directly addresses complaints from U.S. customers. For example, uCloudlink Hong Kong's CEO, Mr. Gao, directed [redacted]

83. Although he was hired by the predecessor to uCloudlink Shenzhen, in fact, Mr. Wang [redacted]

84. Indeed, consistent with the fact that the uCloudlink Group is a single entity made up of several legal contracting entities intended to evade or avoid liability, uCloudlink Hong Kong's CEO, Mr. Gao, admitted [redacted]

JURISDICTION AND VENUE

85. This is an action in law and equity for patent infringement and misappropriation of trade secrets, arising under the United States Patent laws (e.g., 35 U.S.C. § 101 *et seq.*), the Defend Trade Secrets Act of 2016 (e.g., 18 U.S.C. § 1836 *et seq.*), and the Texas Uniform Trade Secrets Act (e.g., TEX. CIV. PRAC. & REM. CODE ANN. § 134A).

86. Therefore, this Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1338, 2201, and 2202.

87. uCloudlink Hong Kong, uCloudlink Shenzhen, and uCloudlink New are each foreign corporations.

88. Therefore, venue is proper in this district pursuant to 28 U.S.C. § 1391 and/or 28 U.S.C. § 1400(b) with respect to uCloudlink Hong Kong, uCloudlink Shenzhen, and uCloudlink New.

89. This Court has personal jurisdiction over uCloudlink Hong Kong, uCloudlink Shenzhen, and uCloudlink New because they, directly and/or through their affiliates and agents, have conducted and conduct business within the United States and Texas, including in this District.

90. Defendants conduct business in Texas and/or in this District involving devices that utilize uCloudlink's Cloud SIM technology and redesigned software, including at least the G2, G3,

G4 and U2 Series WiFi hotspot devices (including variants such as "S" versions), along with the S1 and P3 mobile phones. For example, Defendants sell and/or rent devices in Texas and/or in this this District using Cloud SIM technology under two in-house brands—RoamingMan and GlocalMe.

91. Defendants, also ship, distribute, offer for sale, sell, develop, and enable the use of devices that utilize uCloudlink's Cloud SIM technology indirectly through intermediaries (including distributors, retailers, and others) under different branding and product nomenclature in Texas and/or in this District.

92. Defendants are subject to this Court's specific personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute due at least to their substantial business conducted in this forum, directly and/or through intermediaries, including (i) having solicited business in the State of Texas and in this District, transacted business within the State of Texas and in this District, and attempting to derive financial benefit from residents of the State of Texas and this District, including benefits directly related to the patent infringement and trade secret misappropriation claim set forth herein; (ii) having placed their products and services into the stream of commerce throughout the United States, and enabled and facilitated the use of the same, and having been actively engaged in transacting business in Texas and in this District; and (iii) either alone or in conjunction with others, having committed acts of patent infringement and/or trade secret misappropriation within Texas and in this District, as, on information and belief, uCloudlink Hong Kong, uCloudlink Shenzhen, and uCloudlink New directly and/or through intermediaries, have advertised (including through websites), offered to sell, sold, and/or distributed products that use SIMO and Skyroam's trade secrets and/or Patents, and/or have induced the sale and use of products that use SIMO and Skyroam's trade secrets and/or patents in the United States, Texas,

and this District.

93. uCloudlink Hong Kong, uCloudlink Shenzhen, and uCloudlink New, have, directly or through their distribution network, purposefully and voluntarily placed such products in the stream of commerce knowing and expecting them to be purchased and used by consumers in Texas and in this District.

94. On information and belief, uCloudlink Hong Kong, uCloudlink Shenzhen, and uCloudlink New have contracted with Texas residents for the sale of devices that utilize the uCloudlink Cloud SIM technology, and are therefore within the Texas Long-Arm Statute.

95. On information and belief, uCloudlink Hong Kong entered into a contract in Texas with DHI, a Texas resident (the "uCloudlink-DHI Agreement"). For this additional reason, this Court has personal jurisdiction over uCloudlink Hong Kong.

96. On information and belief, uCloudlink Shenzhen employees [redacted]

97. On information and belief, drafts of the uCloudlink-DHI Agreement were and are in the possession, custody, and/or control of [redacted].

98. On information and belief, uCloudlink Shenzhen [redacted]

99. On information and belief, uCloudlink Shenzhen's [redacted]

[redacted]

100. uCloudlink Shenzhen and uCloudlink New are directly involved with [redacted]s. Thus, uCloudlink Shenzhen and uCloudlink New are involved in [redacted]

101. uCloudlink Shenzhen and uCloudlink New both [redacted]

102. uCloudlink Shenzhen and uCloudlink New are the uCloudlink entities that [redacted] These acts by uCloudlink Shenzhen and uCloudlink New are both to fulfill contracts with Texas residents and are acts constituting torts committed in Texas in the form of patent infringement and/or trade secret misappropriation.

103. In particular, in the New York Patent Case, uCloudlink identified sixteen individuals as being involved in the conception, experimentation, design, development, operation, manufacture, testing, marketing, and/or sale of the uCloudlink devices. Fourteen (14) of those

individuals are employed by [redacted]. Thus, [redacted] is employing individuals to fulfill contracts with Texas residents that are acts constituting torts committed in Texas in the form of patent infringement and/or trade secret misappropriation

104. On information and belief, notwithstanding the fact that the uCloudlink-DHI Agreement was purportedly between [redacted] and DHI, [redacted]

105. On information and belief, uCloudlink Hong Kong, uCloudlink Shenzhen, and uCloudlink New have committed a tort in whole or in part in this state by virtue of their patent infringement and/or trade secret misappropriation as detailed below, and are therefore within the Texas Long-Arm Statute.

106. In particular, uCloudlink Hong Kong, uCloudlink Shenzhen, and uCloudlink New do one or more of the following with the uCloudlink devices that embody SIMO and Skyroam's patented and/or trade secret technology: (a) import these devices into the United States for sale to consumers, including consumers in Texas; (b) sell them or offer them for sale in the United States, including to customers in Texas; (c) sell them to customers who incorporate them into products that such customers import, sell, or offer for sale in the United States, including in Texas; and/or (d) enable and support the use of the uCloudlink devices in the United States, including to customers in Texas.

107. uCloudlink Shenzhen and uCloudlink New also [redacted]

[redacted] constitutes a tort in the form of direct patent infringement and/or trade secret misappropriation, meaning that personal jurisdiction is proper with respect to uCloudlink Shenzhen and uCloudlink New.

108. Finally, because the uCloudlink Group does not differentiate between the uCloudlink entities with respect to corporate formalities and business requirements, personal jurisdiction is proper over all Defendants at least for the reasons given above with regard to uCloudlink Hong Kong.

109. For the above reasons, this Court has personal jurisdiction over each of the Defendants at least because acts of each of the Defendants falls within the Texas Long Arm Statute.

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 9,736,689

110. Plaintiffs incorporate the allegations set forth in the foregoing paragraphs of this Complaint as if fully set forth herein.

111. On August 15, 2017, the United States Patent and Trademark Office duly and legally issued the ’689 Patent, a copy of which is attached as Exhibit A to this Complaint.

112. The ’689 Patent discloses and claims systems, apparatus, and methods for mobile telephone roaming.

113. SIMO is the sole owner and assignee of the ’689 Patent. It owns all rights, title, and interest in and to the ’689 Patent, including all rights to sue and recover for past and future infringement.

114. The ’689 Patent has not expired and is currently in full force and effect.

115. Upon information and belief, Defendants have been and are now directly infringing the ’689 Patent by making, using, selling, and/or offering for sale in the United States and/or importing into the United States WiFi hotspot devices and mobile phones that practice or embody

at least claims 8 and 19 of the '689 Patent. These infringing WiFi hotspot devices and mobile phones include at least the G2, G3, G4 and U2 Series WiFi hotspot devices (including "S" versions), along with the S1 and P3 mobile phones that utilize uCloudlink's redesigned software and those WiFi hotspot devices and mobile phones that were not on the market at the time the Southern District of New York entered judgment of infringement (the "Accused Infringing Products"). Defendants have directly infringed and continue to directly infringe literally and/or under the doctrine of equivalents. Defendants are therefore liable for direct infringement of the '689 Patent under 35 U.S.C. § 271.

116. Upon information and belief, Defendants directly practice at least claims 8 and 19 of the '689 Patent using the Accused Infringing Products through, for example, making, selling, offering for sale, importing, demonstrating, and/or testing of the Accused Infringing Products at least as shown below:

> Back at the conference area at CES 2017, the GlocalMe proved to be of great help, especially at large conferences like CES. It was much easier to use your own wifi hotspot rather than logging in to the provided wifi connection with thousands of people hogging the service.

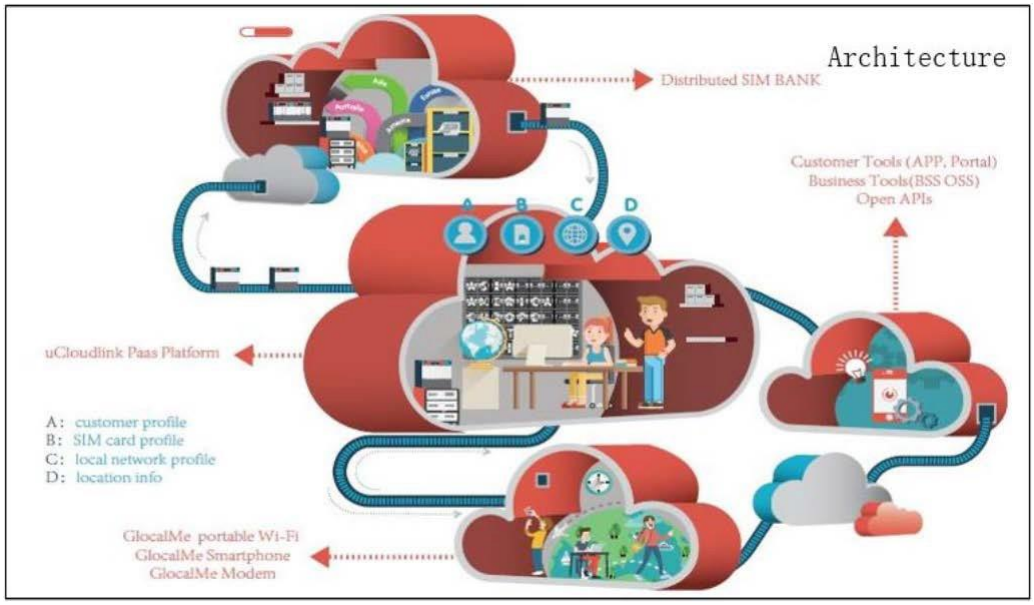
(https://www.glocalme.com/about/newsdetail?id=178)

(https://www.glocalme.com/service/cover)

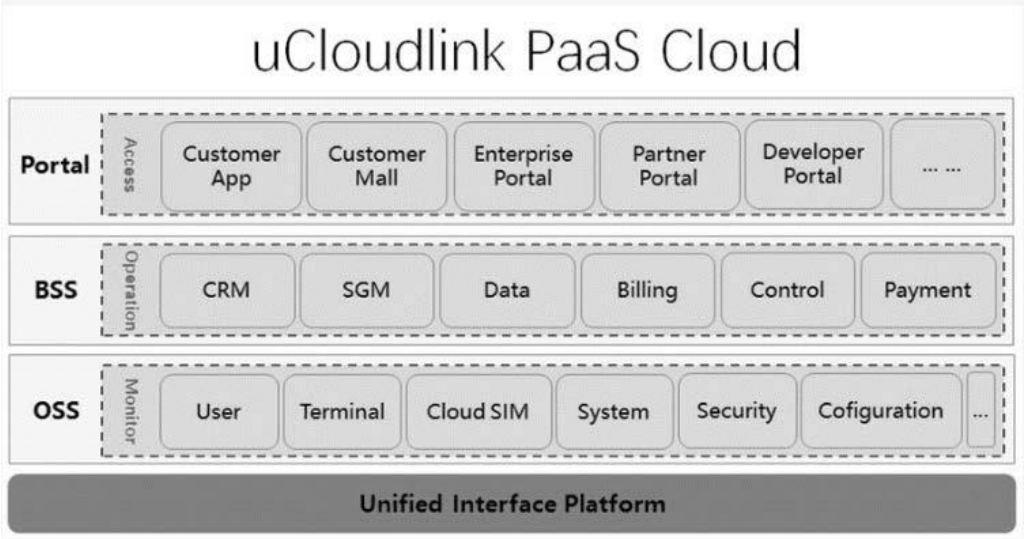
117. Upon information and belief, uCloudlink Hong Kong and/or uCloudlink Shenzhen

will be demonstrating one or more of the Accused Infringing Devices at the Consumer Electronics Show 2020 in Las Vegas, Nevada, on or about January 7, 2020.

118. Upon information and belief, each Accused Infringing Product includes a wireless communication client or extension unit comprising a plurality of memory, processors, programs, communication circuitry, authentication data stored on a subscribed identify module (SIM) card and/or in memory and non-local calls database, at least one of the plurality of programs stored in the memory comprises instructions executable by at least one of the plurality of processors. For example, according to uCloudlink.com, "in addition to operating its own large CloudSIM data centers, uCloudLink also offers smaller 'Local SIM Banks' that partners all over the world can operate locally." (https://www.ucloudlink.com/html/sim-banks/). Further:

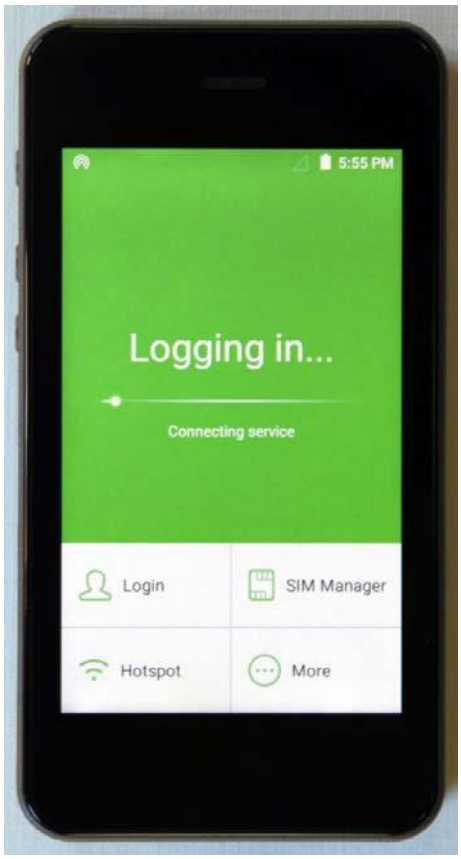


(https://www.ucloudlink.com/html/paas-platform/)



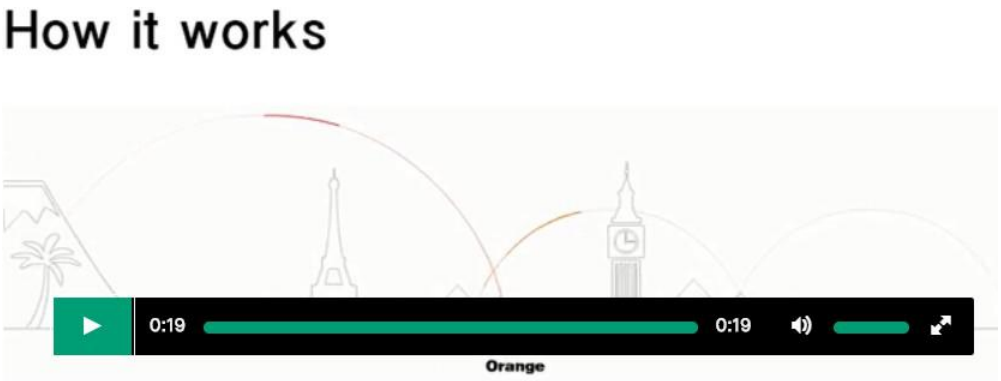
(https://www.ucloudlink.com/html/paas-platform/)

119. Upon information and belief, each Accused Infringing Product practices enabling an initial setting of the wireless communication client or the extension unit and a remote administration system, in addition to establishing a data communication link to transmit information among the wireless communication client or the extension unit, and the remote administration system, as shown below:



(GlocalMe G3).

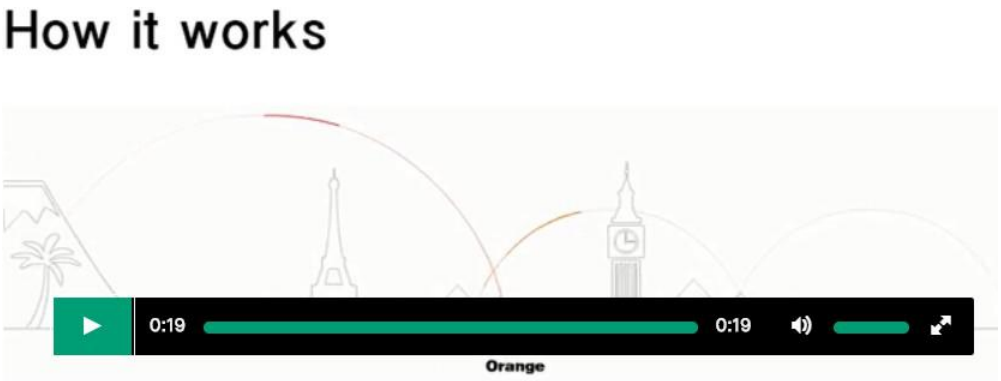
120. Upon information and belief, each Accused Infringing Product practices establishing a local authentication information request in response to a local authentication request by a local cellular communication network, wherein the local authentication information request comprises information regarding the local authentication request for local authentication information received by the foreign wireless communication client or the extension unit from the local cellular communication network, and wherein the data communication link is distinct from the local cellular communication network, as shown below:



(https://www.kickstarter.com/projects/787756203/glocalme-kills-sim-card-and-roaming- pains/description)

(https://www.glocalme.com/mall/wifi?type=g3&giso=US)

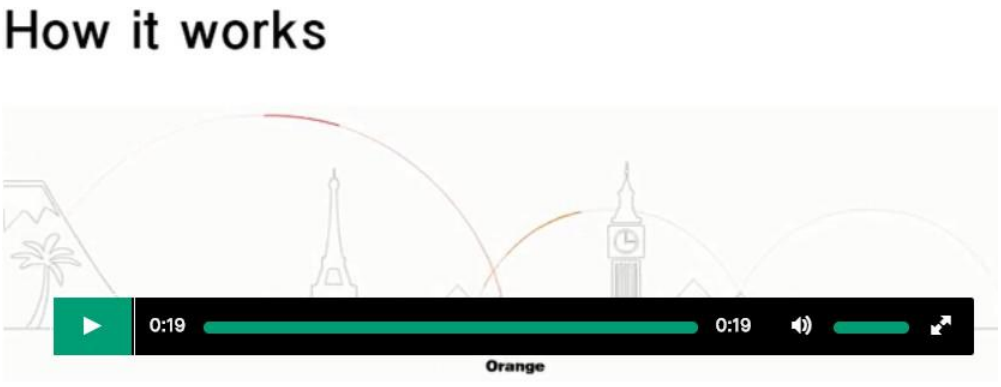
121. Upon information and belief, each Accused Infringing Product practices relaying the local authentication information request to the remote administration system via the data communication link and obtaining suitable local authentication information from the remote administration system via the data communication link, as shown below:



(https://www.kickstarter.com/projects/787756203/glocalme-kills-sim-card-and-roaming- pains/description)

(https://www.glocalme.com/mall/wifi?type=g3&giso=US)

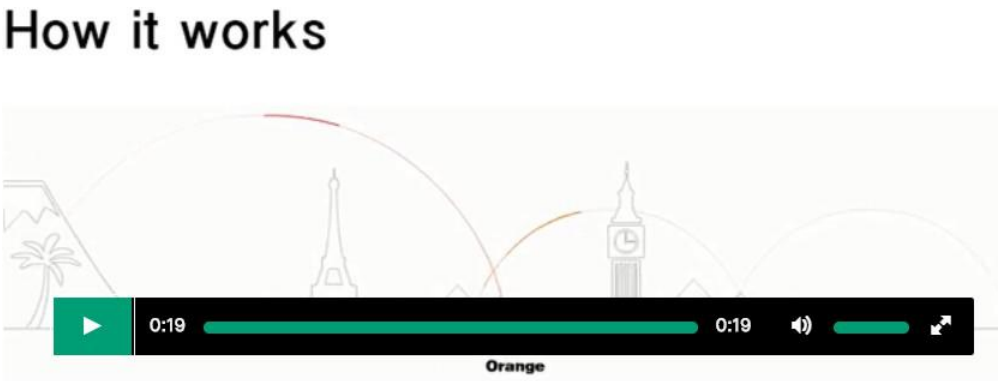
122. Upon information and belief, each Accused Infringing Product practices establishing local wireless services provided by the local cellular communication network to the wireless communication client or the extension unit by sending the local authentication information obtained from the remote administration system to the local cellular communication network over signal link, as shown below:



(https://www.kickstarter.com/projects/787756203/glocalme-kills-sim-card-and-roaming- pains/description)

(https://www.glocalme.com/mall/wifi?type=g3&giso=US)

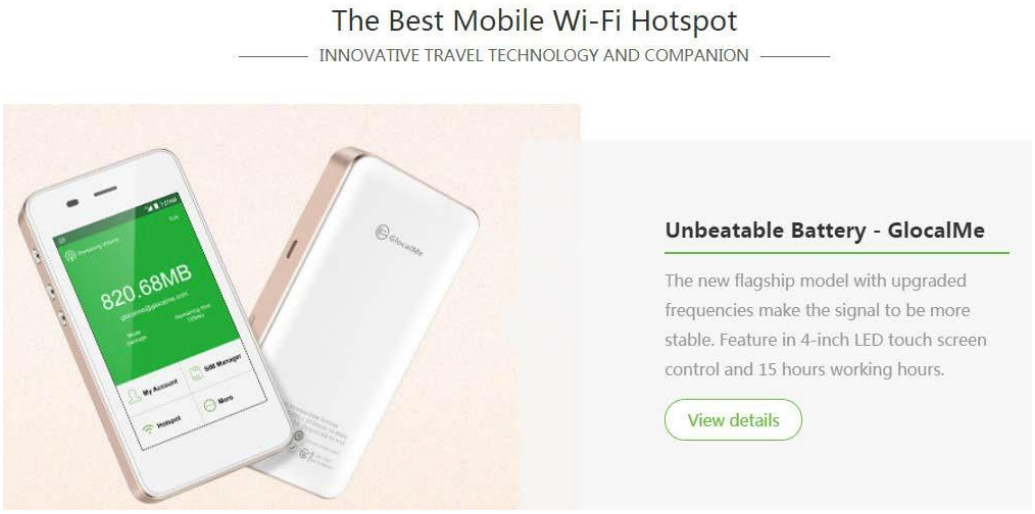
123. Upon information and belief, each Accused Infringing Product practices providing a communication service to the wireless communication client or the extension unit according to the established local wireless services, as shown below:



(https://www.kickstarter.com/projects/787756203/glocalme-kills-sim-card-and-roaming- pains/description)

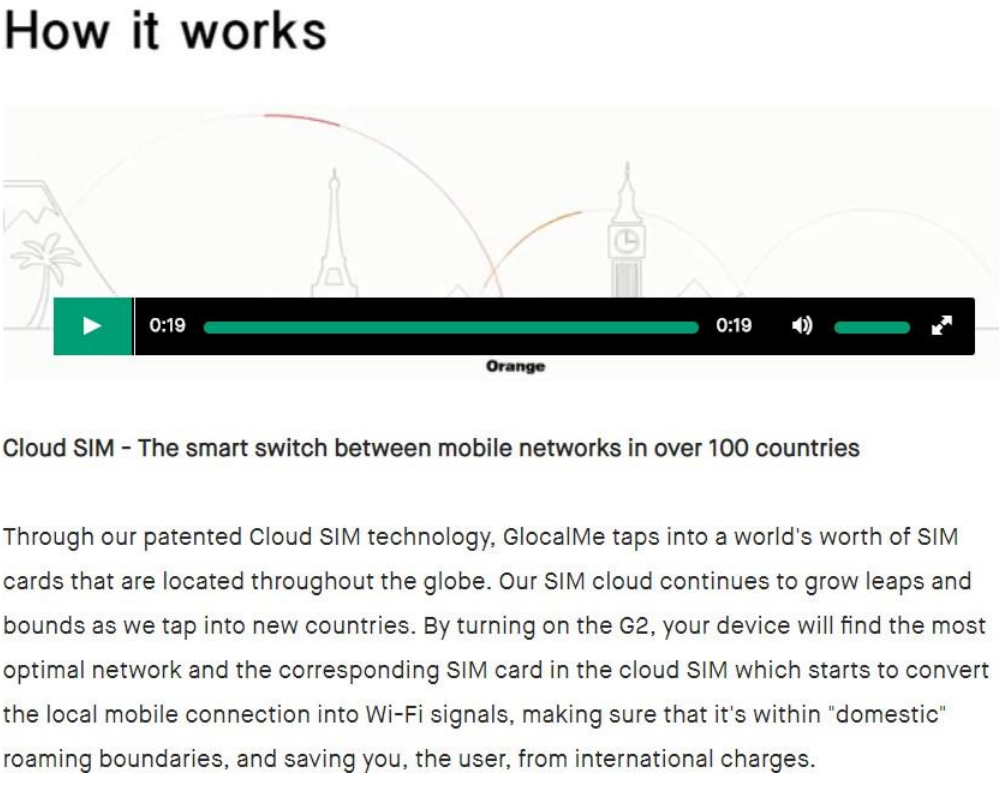
(https://www.glocalme.com/mall/wifi?type=g3&giso=US)

124. Upon information and belief, each Accused Infringing Product practices a method for operating a mobile telecommunications device in a communication network, as shown below:



(https://www.glocalme.com/)

125. Upon information and belief, each Accused Infringing Product practices receiving a first request, via a data channel, for associating a subscriber identity module (SIM) with a mobile telecommunications device, wherein the SIM is subscribed to a local carrier for a current location of the mobile telecommunications device and the mobile telecommunications device is not subscribed to the local carrier, and wherein the first request comprises information regarding a second request from the local carrier received by the mobile telecommunications device over a local cellular communication network for local authentication information, as shown below:

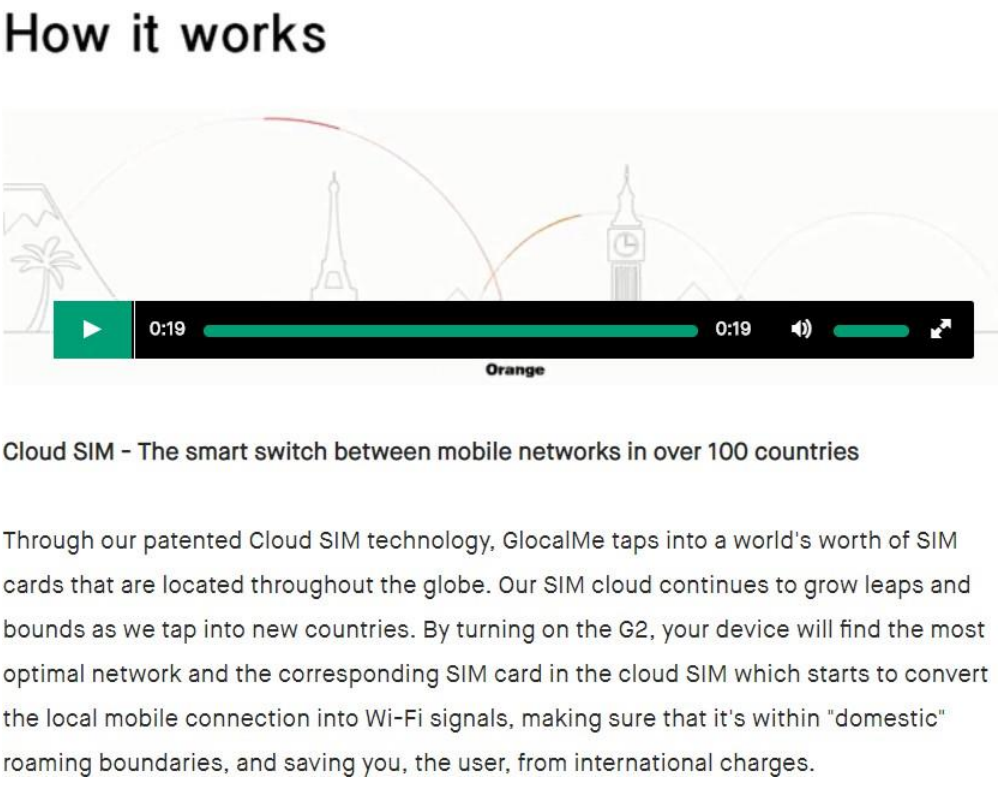


(https://www.kickstarter.com/projects/787756203/glocalme-kills-sim-card-and-roaming-pains/description)

(https://www.glocalme.com/mall/wifi?type=g3&giso=US)

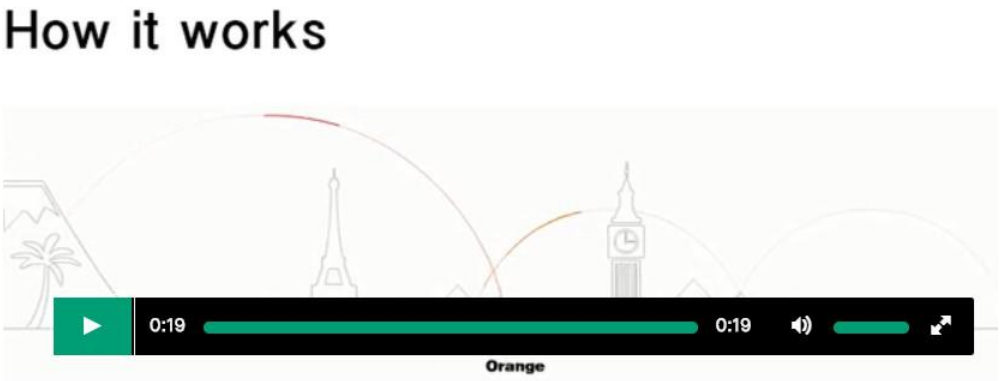
126. Upon information and belief, each Accused Infringing Product practices retrieving authentication information for the mobile telecommunications device from the SIM in response to receiving the first request for associating the SIM with the mobile telecommunications device, as

shown below:



(https://www.kickstarter.com/projects/787756203/glocalme-kills-sim-card-and-roaming- pains/description)

127. Upon information and belief, each Accused Infringing Product practices sending the authentication information to the mobile telecommunications device over the data channel, wherein the data channel is not associated with a local wireless service provided to a subscriber of the local carrier and wherein the authentication information for the mobile telecommunications device retrieved from the SIM is configured to be sent by the foreign wireless communication client or the extension unit to the local carrier over signal link of the local cellular communication network to provision a communication service from the local carrier for the mobile telecommunications device, as shown below:



(https://www.kickstarter.com/projects/787756203/glocalme-kills-sim-card-and-roaming- pains/description)

128. Accordingly, upon information and belief, Defendants have been and are directly infringing claims 8 and 19 of the ’689 Patent either literally or under the doctrine of equivalents. This is true notwithstanding the fact that the Southern District of New York has ruled that the Redesigned Devices are more than colorably different than the Infringing Devices.

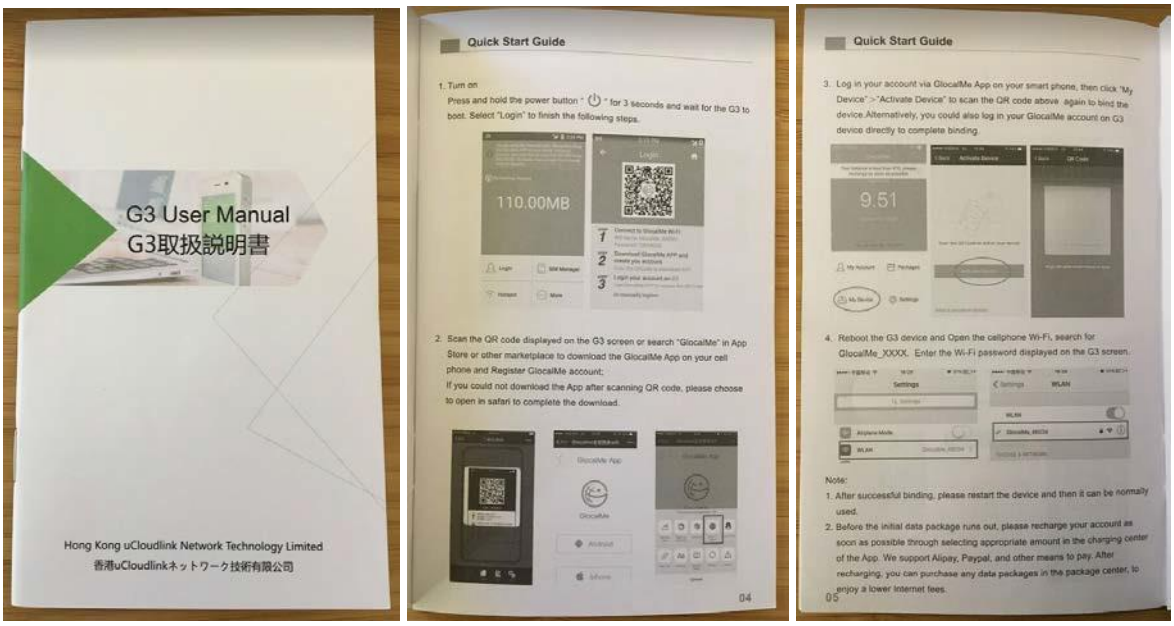
129. Upon information and belief, Defendants also have been and are now indirectly infringing at least claims 8 and 19 of the ’689 Patent either by inducing infringement by others or by contributing to the infringement of others.

130. At least as early as August 13, 2018, Defendants possessed knowledge of the ’689 Patent, and of the fact that sales of their WiFi hotspots and phones infringed the ’689 Patent.

131. Because of this knowledge, Defendants have been and are now actively inducing others, including their distributors, customers and end-users who use, sell, or offer to sell the

Accused Infringing Products, to directly infringe at least claims 8 and 19 of the ’689 Patent.

132. Upon information and belief, Defendants provide and continue to provide manuals, training, guides, videos, and/or demonstrations that induce their distributors, customers and/or end-users to perform acts intended by Defendants to directly infringe the ’689 Patent, for example as shown below:



133. Defendants are therefore liable for inducing infringement of the ’689 Patent under 35 U.S.C. § 271(b).

134. Defendants are also contributing to infringement of at least claims 8 and 19 of the ’689 Patent by others, including their distributors, customers and end-users.

135. Upon information and belief, Defendants contribute to such infringement by providing and continuing to provide the Accused Infringing Products to their distributors, customers and end-users, which are specially made or adapted for use in a manner that infringes the ’689 Patent and are not staple articles of commerce suitable for substantial non-infringing use.

136. Upon information and belief, Defendants have knowledge of the fact that the Accused Infringing Products are specially made or adapted for use to infringe the ’689 Patent and

are not staple articles of commerce suitable for substantial non-infringing use.

137. Defendants are therefore liable for contributory infringement of the ’689 Patent under 35 U.S.C. § 271(c).

138. As a result of their infringement of the ’689 Patent, Defendants have damaged SIMO. Defendants are liable to SIMO in an amount to be determined at trial that adequately compensates SIMO for the infringement, which by law can be no less than a reasonable royalty.

139. Defendants’ acts have caused, and unless restrained and enjoined, will continue to cause, irreparable injury and damage to SIMO for which there is no adequate remedy at law.

140. Upon information and belief, unless enjoined by this Court, Defendants will continue to infringe the ‘689 Patent, directly or indirectly, literally or under the doctrine of equivalents.

UCLOUDLINK’S MISAPPROPRIATION OF PLAINTIFFS’ TRADE SECRETS

Plaintiffs’ Reasonable Measures to Protect their Trade Secrets

141. Plaintiffs’ ability to achieve success in the competitive marketplace hinges on their ability to protect their proprietary information from public disclosure and from further use outside of their business and in particular, by their competitors.

142. Plaintiffs’ trade secrets are not generally known or readily ascertainable nor could they be properly acquired or duplicated by others.

143. Plaintiffs take diligent and reasonable steps to protect their proprietary information. These measures include, by way of example, password protected databases, confidentiality and non-disclosure agreements, and limitations on dissemination of information on a need-to-know basis.

144. To protect their proprietary information internally, Plaintiffs require each employee to review and sign a Technical Non-Disclosure Agreement. The Technical Non-Disclosure

Agreement is signed by the employee on the same date that the employee enters into his or her employment agreement with Plaintiffs.

145. When an employee is terminated or voluntarily discontinues employment with Plaintiffs, he or she must attend an exit interview with management. At such interview, employees are required to return all company-owned items and destroy any and all of Plaintiffs' confidential information in their possession.

146. With regard to third parties, prior to any disclosure of confidential and/or proprietary information, Plaintiffs obligate third parties to sign a non-disclosure agreement. Plaintiffs also mark any document that might be disclosed to a third party under a non-disclosure agreement "CONFIDENTIAL."

147. Plaintiffs take substantial steps to maintain electronic and computer security, as well. For example, Plaintiffs' policies, which are printed and disseminated to their employees, require employees to check documents into the central server upon usage.

148. Further, documents with the highest confidentiality, such as the Skyroam Confidential Documents at issue here, are organized into subsystems. These subsystems are only available to relevant team members who have electronic privileges to view or download.

149. Even more, the SIMO server and computer that host documents of the highest sensitivity, like the Skyroam Confidential Documents, are located in an isolated network that is separate from the entire company's intranet.

150. To protect their electronic systems from outside access, each employee is issued a user name and password, which are required at several different levels to access Plaintiffs' proprietary information. Passwords are required to access different platforms.

151. Finally, Plaintiffs employ several tiers of physical barriers to the access and use of

proprietary and confidential information. For example, to access Plaintiffs' offices, an individual must go through multiple badged doors. Visitors are required to check in and register with a receptionist.

uCloudlink Obtains Confidential Information

152. To Plaintiffs' knowledge at the present time, uCloudlink's misappropriation of Plaintiffs' trade secrets stems primarily from the conduct of former Skyroam employee Mr. Wang. Mr. Wang initially worked at Chinese telecommunications company, Huawei with founders of the uCloudlink Group including Mr. Gao, the CEO and/or sole director of most of the relevant uCloudlink entities, including, but not limited to uCloudlink Cayman, the holding company for all of the uCloudlink entities, uCloudlink Hong Kong, uCloudlink New, and uCloudlink HK.

153. In or about 2011, Mr. Gao joined with several other Huawei colleagues to form the uCloudlink Group.

154. Upon information and belief, in or before 2013, Mr. Gao and the uCloudlink Group became aware of Plaintiffs' developments in the field of virtual SIM technology and viewed Plaintiffs' technology as a threat to the uCloudlink Group's struggling business. With this threat in mind, the uCloudlink Group instituted a series of activities intended to steal and usurp Plaintiffs' intellectual property and improperly leapfrog Plaintiffs' technological and business development capabilities.

155. In early 2013, Mr. Wang left Huawei and joined Skyroam Shenzhen as System Architect. Given the fact that Skyroam was a pioneer in the virtual SIM technology field, Mr. Wang's employment with Skyroam marked his first exposure to any virtual SIM technologies.

156. As a part of his employment, Mr. Wang entered into a Technical Non-Disclosure Agreement with Skyroam. Pursuant to the Technical Non-Disclosure Agreement, Skyroam owns any intellectual property that Mr. Wang created or contributed to during his employment with

Skyroam. The Technical Non-Disclosure Agreement also prohibited Mr. Wang from using any Skyroam confidential information or trade secrets other than for the benefit of Skyroam.

157. Skyroam Shenzhen hired Mr. Wang as its System Architect in the hopes that he could assist Skyroam's top engineers to continue developing its innovative virtual SIM technologies and specifically to help resolve some of the key business problems that Skyroam identified after its core technologies were up and running. In order to do so, Skyroam granted Mr. Wang access to its most sensitive, top secret, confidential, proprietary, and trade secret information. Specifically, Mr. Wang obtained detailed knowledge of Skyroam's confidential, proprietary, and trade secret information and worked with Skyroam's top technical engineers, where he was exposed directly to Skyroam's trade secrets, including but not limited to:

(1) solutions for creating a bank of virtual roaming SIM cards that are used to save substantial fees and improve reliability;

(2) the identification through extensive testing of multiple proprietary inputs to monitor to ensure improved cost savings and reliability in conjunction with the distribution of virtual SIM cards;

(3) the development through extensive testing and utilization of proprietary key performance indicators ("KPI") to determine the most appropriate carrier's card to distribute to a particular customer in a particular location;

(4) a unique and proprietary billing and cost tracking system that differs significantly from methods used by traditional cell phone carriers;

(5) proprietary means for delivering upgrades to devices;

(6) proprietary means for ensuring continued service is available in circumstances where carriers might otherwise cut off service to an end-user;

(7) various proprietary operational procedures related to methods of operating a virtual SIM (vSIM) business including how to operate a SIM bank, crediting accounts, test cases for testing billing systems amongst other operational trade secrets; and

(8) strategic business and marketing development plans to best facilitate the growth of the user network.

158. Moreover, as a system architect, Mr. Wang was exposed to Skyroam's conception, invention, research and development, and reduction to practice of many of Skyroam's technical trade secret solutions described above, especially those involving roaming SIM cards, the allocation of virtual SIM cards based on various parameters, and the design of Skyroam's backend billing systems—key features that enable the successful commercialization of SIMO's patented virtual SIM technology.

159. Several of these processes and techniques to which Mr. Wang was exposed during his employment at Skyroam Shenzhen are Skyroam trade secrets that the uCloudlink Group has misappropriated and continues to misappropriate from Skyroam.

160. Mr. Wang's exposure to these trade secrets is evidenced by email exchanges between Mr. Wang and other members of Skyroam's technical team. In these emails, Skyroam's technical team, including Mr. Wang, discuss the details of these various trade secrets.

161. While employed by Skyroam, Mr. Wang authored numerous specification documents based on information that Skyroam engineers disclosed to him during various meetings. These specifications included many of the Skyroam Confidential Documents that were taken from Skyroam by Mr. Wang and ended up in the possession, custody or control of uCloudlink Hong Kong, uCloudlink America, uCloudlink Shenzhen, and uCloudlink New.

162. Additionally, in his position as a system architect, Mr. Wang had access to a

substantial number of confidential and sensitive documents containing information about Skyroam's trade secrets even beyond the documents that he directly authored.

163. While employed by Skyroam and in direct violation of Skyroam's Technical Non-Disclosure Agreement and electronic usage policies, Mr. Wang copied Skyroam confidential, proprietary and trade secret materials, including but not limited to the Skyroam Confidential Documents, to a USB drive. Mr. Wang subsequently downloaded the Skyroam Confidential Documents to his personal computer and then transferred that information from his personal computer to his uCloudlink work computer.

164. Mr. Wang quit his employment with Skyroam Shenzhen after only four months, in August 2013. Just one month after leaving Skyroam, Mr. Wang joined uCloudlink Shenzhen's predecessor company as a system engineer for testing, maintenance, and technical support of backend servers.

165. Consistent with the fact that the uCloudlink Group views itself as a single entity with a unified business goal, [redacted]

166. At some point while working for an uCloudlink entity, Mr. Wang transferred the stolen Skyroam documents from his personal computer to his uCloudlink work computer, where they ended up in the possession, custody or control of the uCloudlink Group.

167. Upon information and belief, Mr. Wang disclosed at least the substance and content of the Skyroam Confidential Documents to uCloudlink Shenzhen and the broader uCloudlink Group over the course of his employment with the uCloudlink Group.

168. With Mr. Wang's prior knowledge due to his employment at Skyroam Shenzhen

and the benefit of Skyroam's confidential information and trade secrets he took and disclosed during his employment with the uCloudlink Group, uCloudlink was able to accelerate the development of the very same technology.

169. By no coincidence, thanks to the Skyroam trade secret information that Mr. Wang brought over and disclosed to the uCloudlink Group, the uCloudlink Group launched its first virtual SIM product in 2014—merely months after Mr. Wang joined their organization.

170. Mr. Wang was then promoted to the Director of Operation and Maintenance Department to support operation and maintenance of backend servers on September 29, 2014—only one year after joining the uCloudlink Group and only a few months after the uCloudlink Group launched its first commercial product.

171. In March of 2017, Mr. Wang began serving as the leader of the Security Group at uCloudlink Shenzhen, responsible for establishing information security systems, security compliance, and audit.

172. Mr. Wang was referred to as a "[redacted] and evidences the important role Mr. Wang now played at the uCloudlink Group.

The SIMO Trade Secrets

173. Based on the production of the Skyroam Confidential Documents from the New York Patent Case, Plaintiffs have identified several documents in Defendants' possession that contain Skyroam's trade secrets and evidence that Skyroam's trade secrets were, in fact, disclosed to the uCloudlink Group by Mr. Wang.

174. For example, uCloudlink Shenzhen's Chinese patent application, CN105491555A,

discloses the contents of the Skyroam Confidential Documents copied over from Mr. Wang's Skyroam computer to his uCloudlink computer. The patent application lists Mr. Wang and uCloudlink's CEO, Mr. Gao, as co-inventors.

175. Specifically, [redacted], includes large sections that were copied word for word from the stolen Skyroam trade secret document.

176. On October 23, 2015, several uCloudlink employees of different uCloudlink entities, including Mr. Wang [redacted] This exchange also marks a time at which Mr. Wang explicitly disclosed Skyroam's confidential and trade secret information to several other employees of the uCloudlink Group.

177. [redacted]

178. [redacted]

its theft of intellectual property.

179. At this time, if not earlier, these uCloudlink representatives became knowledgeable of the fact that Mr. Wang not only possessed Skyroam's confidential and trade secret information, but that he was willing to share it and intended to use it for the benefit of uCloudlink's similar technology, at least through patent disclosures of which Mr. Wang would purport to be a named inventor.

180. In addition to Mr. Wang, Mr. Gao was named as a co-inventor on the CN105491555A patent application. Remarkably, Mr. Gao agreed to be listed on a patent application where it is demonstrably true that the concept for the patent was lifted word for word from a highly confidential document that Mr. Wang misappropriated from Skyroam.

181. Moreover, despite being named as a co-inventor of this patent application, Mr. Gao [redacted].

182. Under these circumstances Mr. Gao either knew or should have known that the patent application contained technology that Mr. Wang misappropriated from his previous employer—Skyroam.

183. Given [redacted], it is clear that the uCloudlink Group, including uCloudlink Hong Kong, and uCloudlink Shenzhen, knew or should

have known that the technology was not only invented by someone other than the named inventors, but that uCloudlink Shenzhen, through its employee, Mr. Wang, wrongly acquired this confidential information.

184. Although CN105491555A was assigned to uCloudlink Shenzhen, the disclosure of Skyroam's trade secrets in the patent was made with the full knowledge and participation of co-inventor Mr. Gao (who is the CEO and/or director of nearly every relevant uCloudlink entity), uCloudlink Shenzhen's director, David Du, and other uCloudlink Group executives.

185. In addition, the following additional uCloudlink Shenzhen-owned patents and/or applications list Mr. Wang as an inventor and are based on or otherwise include some of Skyroam's stolen trade secrets: CN105282701-A (application publication date: Jan. 27, 2016), CN105228179-A (application publication date: Jan. 6, 2016), CN105979500-A (application publication date: Sept. 28, 2016), CN105813233-A (application publication date: July 27, 2016), CN106211119-A (application publication date: Dec. 7, 2016).

186. With respect to the CN105282701-A application, despite being named as a co-inventor of this patent application, [redacted] he played no role in the invention of the technology, and that he and the uCloudlink Group knew or should have known that the technology was not invented by the named inventors (Mr. Gao and Mr. Wang).

187. Mr. Gao's statements suggest that the uCloudlink Group knew or should have known that the technology was not only invented by someone other than the named inventors, but that uCloudlink Shenzhen through its employee, Mr. Wang, wrongly acquired this confidential information. For example, Mr. Gao [redacted].

[redacted]

188. The lack of evidence of any conception or reduction to practice of any of the inventions allegedly conceived and reduced to practice by Mr. Gao, Mr. Wang, and subsequently assigned to uCloudlink, speaks volumes. Of course [redacted]—they were ***Skyroam's*** and already existed ***word for word*** in ***Skyroam's*** documents.

189. Upon information and belief, the Skyroam Confidential Documents, along with other of Plaintiffs' confidential, proprietary and trade secret information, were discussed by key uCloudlink employees, were the subject of internal uCloudlink implementation documentation so that the Skyroam confidential information could be implemented in uCloudlink's technology (including but not limited to the Accused Infringing Products and the Redesigned Devices), and were used by uCloudlink Shenzhen in patent applications filed in China naming Mr. Wang as one of the inventors.

190. For example, in the New York Patent Action, uCloudlink Hong Kong and uCloudlink America produced documents demonstrating that uCloudlink incorporated Skyroam's non-public confidential information in its own, purportedly confidential internal technical documents. The language and technology in that document is strikingly similar to the language and technology in the Skyroam Confidential Documents, and it discusses Skyroam's top-secret solutions for situations in which the roaming SIM fails or expires. Skyroam did not distribute that information. The only way this information could have ended up in uCloudlink's internal

documentation is if Skyroam's confidential trade secret documents were used as source material.

191. Notably these confidential Skyroam documents were necessarily in the possession, custody or control of uCloudlink Hong Kong and uCloudlink America, as these were the only uCloudlink entities that were parties to the Southern District of New York lawsuit.

192. Not so coincidentally, more than one of the Skyroam Confidential Documents was produced by uCloudlink Hong Kong and uCloudlink America, including documents produced at documents Bates numbered UCLOUDLINK0043869 and UCLOUDLINK0043881.

Mr. Wang

193. In response to SIMO's written discovery requests in the New York Patent Case seeking "documents relating to SIMO," uCloudlink Hong Kong and uCloudlink America produced nearly thirty thousand pages of documents that they had ***in their possession, custody or control.*** Buried in this massive production were at least 14 internal Skyroam documents. Many of these documents were labeled by Skyroam as "Confidentiality Level: Top Secret" and/or bore Skyroam's trademark.

194. The transfer of Skyroam documents from Mr. Wang's personal computer to his uCloudlink computer was not some accidental occurrence or mix up. Mr. Wang later testified under oath that he used a thumb drive to steal the documents from Skyroam and to copy the documents to his home computer and uCloudlink computer.

195. In particular, when asked during his deposition about his theft of the Skyroam Confidential Documents, Mr. Wang initially refused to answer many related questions based on a vague assertion of "personal privacy" on at least 16 different occasions.

196. SIMO moved to compel his testimony over the baseless objection, and the New York District Court granted SIMO's motion. The Court also prohibited counsel for uCloudlink

Hong Kong and uCloudlink America from making any statements other than "objection." Mr. Wang's second day of deposition recommenced several days later, on November 12, 2018.

197. During the second day of his sworn testimony in the New York Patent Case, Mr. Wang's new personal counsel, arranged by uCloudlink Hong Kong and uCloudlink America, advised him on multiple occasions to refuse to answer questions including, among others, those regarding Mr. Wang's theft and use of Skyroam's trade secrets and uCloudlink's involvement or knowledge thereof, based on the Fifth Amendment. Pursuant to such advice, Mr. Wang refused to answer more than forty (40) questions on Fifth Amendment grounds.

198. Mr. Wang's refusal to answer—first on non-existent personal privacy grounds, and then on Fifth Amendment grounds—supports the inference that the uCloudlink Group, through Mr. Wang's testimony, sought to conceal the truth about the uCloudlink Group's improper theft, receipt, use, and/or publication, i.e. misappropriation of Plaintiffs' trade secrets.

199. Upon information and belief, Mr. Wang's refusal to answer questions indicates that he was hiding the scope of his involvement in the theft of Skyroam's trade secrets and covering up the extent to which others at uCloudlink were involved with the theft, receipt, disclosure and/or use of Skyroam's trade secrets.

200. Since at least the beginning of Mr. Wang's employment with uCloudlink, when the Skyroam trade secrets and confidential information were first disclosed to employees of the uCloudlink Group, the uCloudlink entities have actively used Skyroam's technology, including its trade secrets to unfairly compete with Skyroam.

201. Additionally and independent of the uCloudlink Group's and uCloudlink Shenzhen's further disclosure and use of Skyroam's trade secrets, Mr. Wang intentionally, willfully, and maliciously misappropriated Skyroam's trade secrets when he accessed the

documents by improper means (in violation of his employment agreement and numerous Skyroam policies), and disclosed and used the technology therein in the ordinary scope of his duties as an employee of uCloudlink Shenzhen and the uCloudlink Group for the benefit of uCloudlink Shenzhen and the uCloudlink Group to create and develop the uCloudlink Group's products and technology, and to disclose the trade secrets in uCloudlink Group patents.

202. The uCloudlink Group and uCloudlink Shenzhen knew or should have known that a high level technical employee hired directly from a competitor in a two-player market to take on a similar role under uCloudlink's employment inevitably resulted or would result in Mr. Wang and/or the uCloudlink Group and uCloudlink Shenzhen disclosing and/or using those trade secrets to compete with Skyroam.

203. Upon information and belief, the uCloudlink Group has developed its business on the theft and improper disclosure and use of technology developed by others—in this case, Skyroam. At the very least Mr. Wang's misappropriation was reasonably foreseeable by the uCloudlink Group and, in particular, uCloudlink Shenzhen. Thus, uCloudlink Shenzhen and the uCloudlink Group are vicariously liable for Mr. Wang's improper use and disclosure of Skyroam's trade secrets under the doctrines of agency and *respondeat superior*.

204. uCloudlink's theft, receipt, use, and disclosure of Plaintiffs' trade secrets are not limited to the acts of Mr. Wang.

205. On July 3, 2016, uCloudlink Hong Kong's President of Global Partner Business, William Li, [redacted] uCloudlink Shenzhen a confidential 2015 Skyroam marketing document regarding Skyroam's partnership business model ("Confidential Skyroam Marketing Materials"). Mr. Li, uCloudlink Hong Kong's President of Global Partner Business, directed uCloudlink Shenzhen [redacted].

206. The Confidential Skyroam Marketing Materials are marked "confidential" on every page of the document. No Skyroam entity approved the sending of this document to any uCloudlink entity.

207. On April 25, 2017, [redacted].

208. Because of the confidential nature of Confidential Skyroam Marketing Materials, uCloudlink Shenzhen, uCloudlink Hong Kong, and/or uCloudlink New, by virtue of the actions of their employees, William Li, Zeng Rongrong, and any other uCloudlink Hong Kong, uCloudlink Shenzhen, or uCloudlink New employees that received this the Confidential Skyroam Marketing Materials knew or should have known that the document contained Plaintiffs' confidential trade secrets and that those trade secrets were wrongly acquired by uCloudlink Hong Kong and uCloudlink Shenzhen.

209. The Skyroam Confidential Documents and Confidential Skyroam Marketing Document produced by uCloudlink Hong Kong and uCloudlink America in the New York Patent Case reveal trade secrets that include, but are not limited to: (1) solutions for creating a bank of virtual roaming SIM cards that are used to save substantial fees and improve reliability; (2) the identification through extensive testing of multiple proprietary inputs to monitor to ensure improved cost savings and reliability in conjunction with the distribution of virtual SIM cards; (3) the development through extensive testing and utilization of proprietary key performance indicators ("KPI") to determine the most appropriate carrier's card to distribute to a particular customer in a particular location; (4) a unique and proprietary billing and cost tracking system that differs significantly from methods used by traditional cell phone carriers; (5) proprietary means

for delivering upgrades to devices; (6) proprietary means for ensuring continued service is available in circumstances where carriers might otherwise cutoff service to an end-user; (7) various proprietary operational procedures related to methods of operating a vSIM business including how to operate a SIM bank, crediting accounts, test cases for testing billing systems amongst other operational trade secrets; and (8) strategic business and marketing development plans to best facilitate the growth of the user network.

210. uCloudlink's use of such information has caused and will continue to cause substantial and irreparable injury to Skyroam. Such harm includes, and is not limited to, shortening the runway for uCloudlink to develop and release its virtual SIM platform and mobile hotspots. Moreover, the disclosure and use of this confidential information enabled uCloudlink to raise investment dollars and present a marketing strategy that was developed, in significant part, not by uCloudlink, but by Skyroam.

211. The uCloudlink Group continues to misappropriate Skyroam's trade secrets by selling products and services developed using Skyroam's trade secrets and that incorporate and embody Skyroam's trade secret technology.

212. Skyroam brings this action to halt and remedy the intentional dissemination and use of their intellectual property, in violation of federal and state trade secret misappropriation laws and the federal patent laws of the United States.

COUNT II
MISAPPROPRIATION OF TRADE SECRETS UNDER
THE DEFEND TRADE SECRETS ACT (18 U.S.C. § 1836(b)(1))

213. Plaintiffs incorporate the allegations set forth in the foregoing paragraphs of this Complaint as if fully set forth herein.

214. The Defend Trade Secrets Act (the "DTSA") provides a federal private cause of action for "[a]n owner of a trade secret that is misappropriated . . . if the trade secret is related to a

product or service used in, or intended for use in, interstate or foreign commerce." 18 U.S.C. § 1836(b)(1). It authorizes courts "to grant an injunction" to "prevent any actual or threatened misappropriation," including by "requiring affirmative actions . . . to protect the trade secret." *Id.* at § 1836(b)(3)(A)(i)–(ii).

215. Under the DTSA, "trade secret" means "all forms and types of financial, business, scientific, technical, economic, or engineering information, including . . . formulas, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored," if (A) the trade-secret owner "has taken reasonable measures to keep such information secret," and (B) "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information." *Id.* at § 1839(3).

216. Plaintiffs are the owner of trade secrets that include, but are not limited to (1) solutions for creating a bank of virtual roaming SIM cards that are used to save substantial fees and improve reliability; (2) the identification through extensive testing of multiple proprietary inputs to monitor to ensure improved cost savings and reliability in conjunction with the distribution of virtual SIM cards; (3) the development through extensive testing and utilization of proprietary key performance indicators ("KPI") to determine the most appropriate carrier's card to distribute to a particular customer in a particular location; (4) a unique and proprietary billing and cost tracking system that differs significantly from methods used by traditional cell phone carriers; (5) proprietary means for delivering upgrades to devices; (6) proprietary means for ensuring continued service is available in circumstances where carriers might otherwise cutoff service to an end-user; (7) various proprietary operational procedures related to methods of

operating a vSIM business including how to operate a SIM bank, crediting accounts, test cases for testing billing systems amongst other operational trade secrets; and (8) strategic business and marketing development plans to best facilitate the growth of the user network.

217. Plaintiffs' trade secrets are not generally known or readily ascertainable nor could they be properly acquired or duplicated by others. Plaintiffs' trade secrets indisputably contribute to the monumental success Plaintiffs have seen in the last ten years, making Plaintiffs a top choice amongst their 15 million users worldwide including travelers from the Americas, Europe, and Asia.

218. As alleged in the foregoing paragraphs, at all times, Plaintiffs have taken reasonable and extensive efforts to keep their trade secrets secret through the use of Nondisclosure and Confidentiality Agreements, employment agreements, and employee training. All of Plaintiffs' trade secrets are stored on secure servers and are password-protected. Additionally, technical documents containing Plaintiffs' trade secrets are clearly and consistently marked "Confidentiality: Top Secret," and certain confidential marketing documents are clearly and consistently marked "Confidential."

219. Plaintiffs' trade secrets have independent economic value. Since 2008, Plaintiffs have invested and continue to invest millions of dollars into research and development and implementation of the trade secret protected systems, including their hotspot devices. Plaintiffs have also invested and continue to invest significant economic resources into refining their products and marketing their products and services in order to increase the adoption of their devices by users thereby increasing the functionality and stability of its platform.

220. Plaintiffs' trade secrets are crucial to the success of the implementation, operation, and maintenance of Plaintiffs' proprietary technology, and business development. They provide a

decisive competitive advantage to Plaintiffs and to anyone else with access to this information. Plaintiffs' trade secrets provide the company with a critical market advantage in attracting new customers, based on their connection speed and reliability, for example.

221. Plaintiffs have devoted the bulk of their research and development efforts to create the most efficient and effective solution for optimizing the vSIM technology.

222. These trade secrets derive independent value because they significantly increase the usability, reliability, and consistency of the connections required for mobile hotspot users through vSIM technology.

223. Indeed, Plaintiffs have conducted cost/benefit analyses surrounding these very trade secrets and has concluded that their implementation is vital to the profitability of their business.

224. Plaintiffs' ability to achieve success in the competitive marketplace hinges on their ability to protect their proprietary information from public disclosure and from further use outside of Plaintiffs and in particular, by their competitors.

225. At no time did Plaintiffs consent to Mr. Wang, uCloudlink Shenzhen, and/or uCloudlink Hong Kong's improper acquisition, use, or disclosure of its trade secrets or confidential information for any purpose. Rather, Mr. Wang stole Plaintiffs' trade secrets by improper means and in explicit violation of his Technical Non-Disclosure Agreement.

226. Indeed, Mr. Wang acquired Skyroam's trade secrets through a relationship of trust, in which he signed a Technical Non-Disclosure Agreement and an Employment Agreement that imposed upon him a duty to maintain the confidentiality of Skyroam's confidential information and trade secrets and to not improperly use and/or disclose the same.

227. As alleged in the foregoing paragraphs, at least uCloudlink Hong Kong and

uCloudlink Shenzhen wrongfully acquired the Skyroam's commercial trade secrets in the form of the Confidential Skyroam Marketing Materials. At least uCloudlink Hong Kong, uCloudlink Shenzhen, and any other uCloudlink entity that received the Confidential Skyroam Marketing Materials knew or had reason to know that the document circulated by their employees, at least William Li and Rongrong Zeng, was improperly acquired by uCloudlink Hong Kong and uCloudlink Shenzhen.

228. uCloudlink Shenzhen knew or had reason to know that its employee, Mr. Wang improperly acquired Skyroam's trade secrets from Skyroam while knowing or having a reason to know that Mr. Wang owed a duty to Skyroam to maintain the information in secrecy.

229. Moreover, uCloudlink Shenzhen's misappropriation of Skyroam's trade secrets stems not only from its improper acquisition of Skyroam's trade secrets, but also in its improper disclosure and use of those trade secrets. For example, uCloudlink Shenzhen has applied for at least 6 Chinese patents listing Mr. Wang as inventor that, on information and belief, disclose Skyroam's trade secrets that uCloudlink conspired with Mr. Wang to steal from Skyroam: CN105491555-A (application publication date: April 13, 2016), CN105282701-A (application publication date: Jan. 27, 2016), CN105228179-A (application publication date: Jan. 6, 2016), CN105979500-A (application publication date: Sept. 28, 2016), CN105813233-A (application publication date: July 27, 2016), CN106211119-A (application publication date: Dec. 7, 2016). At least two of these patents— CN105282701-A and CN105228179-A—issued on September 25, 2018.

230. By virtue of at least the fact that Mr. Gao, the CEO of uCloudlink Hong Kong, uCloudlink New, and other uCloudlink entities, knew he was not the inventor of certain of the Bin Patents upon which he is a named inventor, at least uCloudlink Hong Kong, and uCloudlink New

knew or should have known that the technology disclosed in those patents and applications was improperly acquired, used, and disclosed by at least uCloudlink Hong Kong and uCloudlink New, and that the same belonged to Skyroam.

231. Notwithstanding uCloudlink Hong Kong, uCloudlink Shenzhen, and uCloudlink New's knowledge that the Confidential Skyroam Marketing Materials were confidential, and wrongly acquired, from Skyroam, uCloudlink improperly used the Confidential Skyroam Marketing Materials to develop and grow its business model using Skyroam's proprietary strategies and plans.

232. Upon information and belief, because of the singular nature of the uCloudlink Group, uCloudlink Hong Kong knew of and/or participated in the misappropriation of Skyroam's trade secrets.

233. Upon information and belief, by the time uCloudlink Hong Kong became the owner and controller of the uCloudlink Group, uCloudlink Hong Kong knew or had reason to know uCloudlink Shenzhen misappropriated Skyroam's trade secrets and that those trade secrets are the foundation for the entire business of the uCloudlink Group and are responsible for the uCloudlink Group's continued viability.

234. For example, the uCloudlink Group offers for sale, and sells products and services that embody the Bin Patents, and therefore, are based, at least in part, on Skyroam's trade secrets and the Skyroam Confidential Documents.

235. Misappropriation Defendants' misappropriation also concerns "product[s] and service[s] used in, or intended for use in interstate or foreign commerce," pursuant to the Defend Trade Secrets Act. Upon information and belief, Misappropriation Defendants knowingly offer for sale, sell, and enable the use of products that embody Skyroam's trade secrets, and therefore, are

based, at least in part, on Skyroam's trade secrets and the Skyroam Confidential Documents, throughout the United States.

236. Specifically Misappropriation Defendants' acts are in furtherance of misappropriation that harms Skyroam in the United States, and specifically causes harm to Skyroam, Inc., which is incorporated under the laws of the state of California with a principle place of business at 180 Sansome Street, Suite 200, San Francisco, CA 94104.

237. Not only are the Misappropriation Defendants' products sold to United States customers in direct competition with Skyroam, but in addition, Misappropriation Defendants' customers who purchased products outside of the United States use these products and connect to Misappropriation Defendants' servers when travelling within the United States. Enabling such connections is a core feature and functionality of the misappropriated trade secrets as well as both the Skyroam's and Misappropriation Defendants' competing products.

238. This conduct is not only based on Plaintiffs' trade secrets but it also takes place in the United States and affects United States customers and a United States corporation.

239. Misappropriation Defendants' manufacture, offers for sale, sales, and enabled use of the products that embody Plaintiffs' trade secrets is ongoing.

240. Misappropriation Defendants have also intentionally, willfully, and maliciously misused trade secrets and/or confidential or proprietary information or knowledge of Plaintiffs and continue to do so. Misappropriation Defendants' use of Skyroam's trade secrets was the result of discovery by improper means by uCloudlink Shenzhen employee Mr. Wang.

241. Skyroam has now discovered evidence that Mr. Wang (1) acquired Plaintiffs' trade secrets by improper means when he copied them onto a USB drive without permission from anyone at Plaintiffs; (2) transferred some or all of the contents of the USB drive copies to his

personal home computer; (3) further copied Plaintiffs' trade secrets to his uCloudlink work computer; (4) disclosed Plaintiffs' trade secrets to other uCloudlink employees at various uCloudlink entities—including, but not limited to, the senior executives at Misappropriation Defendants who are listed as co-inventors on the uCloudlink patents that disclose Plaintiffs' trade secrets; (5) and authored patents now assigned to uCloudlink Shenzhen, founded upon Plaintiffs' trade secrets and confidential and proprietary information—all of which have resulted in the manufacture, offer for sale, and sale of products that embody Plaintiffs' trade secrets in the United States.

242. Misappropriation Defendants subsequently used this information in connection with its business activities, in a manner adverse to Plaintiffs' business interests. Such use was and is without Plaintiffs' express or implied consent.

243. uCloudlink Shenzhen's act of listing senior executives of the uCloudlink Group, including but not limited to its CEO, on patent applications that contain Plaintiffs' misappropriated trade secrets is evidence that the uCloudlink Group knew or had reason to know that its employee, Mr. Wang, improperly obtained Plaintiffs' trade secrets. It is further evidence that the uCloudlink Group knew or should have known that any use of those trade secrets was unauthorized and such use would result in the Misappropriation Defendants competing with and misappropriating Plaintiffs' trade secrets.

244. uCloudlink Hong Kong, uCloudlink Shenzhen, and/or uCloudlink New should be held responsible for the acts of Mr. Wang under the theory of *respondeat superior*.

245. In particular, upon information and belief, Mr. Wang was acting within the scope of his eventual employment by uCloudlink entities at the time he misappropriated Skyroam's trade secrets.

246. Upon information and belief, Mr. Wang was acting in furtherance of uCloudlink's business at the time he misappropriated Skyroam's trade secrets.

247. Upon information and belief, Mr. Wang accomplished an objective for which he was employed relating to developing uCloudlink's cloud-SIM business at the time he misappropriated Skyroam's trade secrets.

248. uCloudlink Hong Kong, uCloudlink Shenzhen, and/or uCloudlink New should be held responsible for the acts of Mr. Wang because at least those three corporate entities and Mr. Wang were engaged in a civil conspiracy.

249. In particular, upon information and belief, the acts of Defendants and Mr. Wang were by two or more persons. These acts were in further of an object to be accomplished in the form of developing uCloudlink's cloud-SIM business. Upon information and belief, Mr. Wang and the Defendants had a meeting of the minds as to the course of action in the form of Mr. Wang obtaining Skyroam confidential information before returning to uCloudlink. Upon information and belief, Mr. Wang committed one or more unlawful overt acts in taking Skyroam's confidential information.

250. Damages were at least one proximate result of Mr. Wang's acts in taking Skyroam's confidential information.

251. As a result, in violation of Plaintiffs' rights, Misappropriation Defendants misappropriated, and continue to use, Plaintiffs' trade secret information in the improper and unlawful manner described above. Misappropriation Defendants' misappropriation of Plaintiffs' confidential, proprietary, and trade secret information was intentional, knowing, willful, malicious, fraudulent, and oppressive. Misappropriation Defendants have further attempted to and continue to attempt to conceal their misappropriation.

252. Misappropriation Defendants' possession, disclosure, and use of Plaintiffs' trade secrets in the back end systems and the same products accused of patent infringement in the instant litigation is the quintessential example of behavior that rises to the level of "willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant, or—indeed—characteristic of a pirate."

253. As the direct and proximate result of Misappropriation Defendants' conduct in the United States, Plaintiffs have suffered and, if Misappropriation Defendants' conduct is not stopped, will continue to suffer, severe competitive harm, irreparable injury, and significant damages, in an amount to be proven at trial. Because Plaintiffs' remedy at law is inadequate, Plaintiffs seek, in addition to damages, injunctive relief to recover and protect their confidential, proprietary, and trade secret information and to protect other legitimate business interests. Plaintiffs' business operates in a highly competitive market and will continue suffering irreparable harm absent injunctive relief.

254. Plaintiffs have been damaged by all of the foregoing and are entitled to an award of exemplary damages and attorneys' fees.

COUNT III
MISAPPROPRIATION OF TRADE SECRETS UNDER THE TEXAS UNIFORM TRADE SECRETS ACT (TEX. CIV. PRAC. & REM. CODE ANN. § 134A)

255. Plaintiffs incorporate the allegations set forth in the foregoing paragraphs of this Complaint as if fully set forth herein.

256. Under the Texas Uniform Trade Secrets Act, TEX. CIV. PRAC. & REM. CODE ANN. § 134A, "trade secret" means "all forms and types of information, including business, scientific, technical, economic, or engineering information, and any formula, design, prototype, pattern, plan, compilation, program device, program, code, device, method, technique, process, procedure, financial data, or list of actual or potential customers or suppliers, whether tangible or intangible and

whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if: (A) the owner of the trade secret has taken reasonable measures under the circumstances to keep the information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

257. Plaintiffs are the owner of trade secrets that include, but are not limited to (1) solutions for creating a bank of virtual roaming SIM cards that are used to save substantial fees and improve reliability; (2) the identification through extensive testing of multiple proprietary inputs to monitor to ensure improved cost savings and reliability in conjunction with the distribution of virtual SIM cards; (3) the development through extensive testing and utilization of proprietary key performance indicators ("KPI") to determine the most appropriate carrier's card to distribute to a particular customer in a particular location; (4) a unique and proprietary billing and cost tracking system that differs significantly from methods used by traditional cell phone carriers; (5) proprietary means for delivering upgrades to devices; (6) proprietary means for ensuring continued service is available in circumstances where carriers might otherwise cutoff service to an end-user; (7) various proprietary operational procedures related to methods of operating a vSIM business including how to operate a SIM bank, crediting accounts, test cases for testing billing systems amongst other operational trade secrets; and (8) strategic business and marketing development plans to best facilitate the growth of the user network.

258. Plaintiffs' trade secrets are not generally known or readily ascertainable nor could they be properly acquired or duplicated by others. Plaintiffs' trade secrets indisputably contribute to the monumental success Plaintiffs have seen in the last ten years, making Plaintiffs a top choice amongst their 15 million users worldwide including travelers from the Americas, Europe, and

Asia.

259. As alleged in the foregoing paragraphs, at all times, Plaintiffs have taken reasonable and extensive efforts to keep their trade secrets secret through the use of Nondisclosure and Confidentiality Agreements, employment agreements, and employee training. All of Plaintiffs' trade secrets are stored on secure servers and are password-protected. Additionally, technical documents containing Plaintiffs' trade secrets are clearly and consistently marked "Confidentiality: Top Secret," and certain confidential marketing documents are clearly and consistently marked "Confidential."

260. Plaintiffs' trade secrets have independent economic value. Since 2008, Plaintiffs have invested and continue to invest millions of dollars into research and development and implementation of the trade secret protected systems, including their hotspot devices. Plaintiffs have also invested and continue to invest significant economic resources into refining their products and marketing their products and services in order to increase the adoption of their devices by users thereby increasing the functionality and stability of its platform.

261. Plaintiffs' trade secrets are crucial to the success of the implementation, operation, and maintenance of Plaintiffs' proprietary technology, and business development. They provide a decisive competitive advantage to Plaintiffs and to anyone else with access to this information. Plaintiffs' trade secrets provide the company with a critical market advantage in attracting new customers, based on their connection speed and reliability, for example.

262. Plaintiffs have devoted the bulk of their research and development efforts to create the most efficient and effective solution for optimizing the vSIM technology.

263. These trade secrets derive independent value because they significantly increase the usability, reliability, and consistency of the connections required for mobile hotspot users

through vSIM technology.

264. Indeed, Plaintiffs have conducted cost/benefit analyses surrounding these very trade secrets and has concluded that their implementation is vital to the profitability of their business.

265. Plaintiffs' ability to achieve success in the competitive marketplace hinges on their ability to protect their proprietary information from public disclosure and from further use outside of Plaintiffs and in particular, by their competitors.

266. At no time did Plaintiffs consent to Mr. Wang, uCloudlink Shenzhen, and/or uCloudlink Hong Kong's improper acquisition, use, or disclosure of its trade secrets or confidential information for any purpose. Rather, Mr. Wang stole Plaintiffs' trade secrets by improper means and in explicit violation of his Technical Non-Disclosure Agreement.

267. Indeed, Mr. Wang acquired Skyroam's trade secrets through a relationship of trust, in which he signed a Technical Non-Disclosure Agreement and an Employment Agreement that imposed upon him a duty to maintain the confidentiality of Skyroam's confidential information and trade secrets and to not improperly use and/or disclose the same.

268. As alleged in the foregoing paragraphs, at least uCloudlink Hong Kong and uCloudlink Shenzhen wrongfully acquired the Skyroam's commercial trade secrets in the form of the Confidential Skyroam Marketing Materials. At least uCloudlink Hong Kong, uCloudlink Shenzhen, and any other uCloudlink entity that received the Confidential Skyroam Marketing Materials knew or had reason to know that the document circulated by their employees, at least William Li and Rongrong Zeng, was improperly acquired by uCloudlink Hong Kong and uCloudlink Shenzhen.

269. uCloudlink Shenzhen knew or had reason to know that its employee, Mr. Wang

improperly acquired Skyroam's trade secrets from Skyroam while knowing or having a reason to know that Mr. Wang owed a duty to Skyroam to maintain the information in secrecy.

270. Moreover, uCloudlink Shenzhen's misappropriation of Skyroam's trade secrets stems not only from its improper acquisition of Skyroam's trade secrets, but also in its improper disclosure and use of those trade secrets. For example, uCloudlink Shenzhen has applied for at least 6 Chinese patents listing Mr. Wang as inventor that, on information and belief, disclose Skyroam's trade secrets that uCloudlink conspired with Mr. Wang to steal from Skyroam: CN105491555-A (application publication date: April 13, 2016), CN105282701-A (application publication date: Jan. 27, 2016), CN105228179-A (application publication date: Jan. 6, 2016), CN105979500-A (application publication date: Sept. 28, 2016), CN105813233-A (application publication date: July 27, 2016), CN106211119-A (application publication date: Dec. 7, 2016). At least two of these patents— CN105282701-A and CN105228179-A—issued on September 25, 2018.

271. By virtue of at least the fact that Mr. Gao, the CEO of uCloudlink Hong Kong, uCloudlink New, and other uCloudlink entities, knew he was not the inventor of certain of the Bin Patents upon which he is a named inventor, at least uCloudlink Hong Kong, and uCloudlink New knew or should have known that the technology disclosed in those patents and applications was improperly acquired, used, and disclosed by at least uCloudlink Hong Kong and uCloudlink New, and that the same belonged to Skyroam.

272. Notwithstanding uCloudlink Hong Kong, uCloudlink Shenzhen, and uCloudlink New's knowledge that the Confidential Skyroam Marketing Materials were confidential, and wrongly acquired, from Skyroam, uCloudlink improperly used the Confidential Skyroam Marketing Materials to develop and grow its business model using Skyroam's proprietary

strategies and plans.

273. Upon information and belief, because of the singular nature of the uCloudlink Group, uCloudlink Hong Kong knew of and/or participated in the misappropriation of Skyroam's trade secrets.

274. Upon information and belief, by the time uCloudlink Hong Kong became the owner and controller of the uCloudlink Group, uCloudlink Hong Kong knew or had reason to know uCloudlink Shenzhen misappropriated Skyroam's trade secrets and that those trade secrets are the foundation for the entire business of the uCloudlink Group and are responsible for the uCloudlink Group's continued viability.

275. For example, the uCloudlink Group offers for sale, and sells products and services that embody the Bin Patents, and therefore, are based, at least in part, on Skyroam's trade secrets and the Skyroam Confidential Documents.

276. Specifically Misappropriation Defendants' acts are in furtherance of misappropriation that harms Skyroam in the United States, and specifically causes harm to Skyroam, Inc., which is incorporated under the laws of the state of California with a principle place of business at 180 Sansome Street, Suite 200, San Francisco, CA 94104.

277. Not only are the Misappropriation Defendants' products sold to United States customers in direct competition with Skyroam, but in addition, Misappropriation Defendants' customers who purchased products outside of the United States use these products and connect to Misappropriation Defendants' servers when travelling within the United States. Enabling such connections is a core feature and functionality of the misappropriated trade secrets as well as both the Skyroam's and Misappropriation Defendants' competing products.

278. This conduct is not only based on Plaintiffs' trade secrets but it also takes place in

the United States and affects United States customers and a United States corporation.

279. Misappropriation Defendants' manufacture, offers for sale, sales, and enabled use of the products that embody Plaintiffs' trade secrets is ongoing.

280. Misappropriation Defendants have also intentionally, willfully, and maliciously misused trade secrets and/or confidential or proprietary information or knowledge of Plaintiffs and continue to do so. Misappropriation Defendants' use of Skyroam's trade secrets was the result of discovery by improper means by uCloudlink Shenzhen employee Mr. Wang.

281. Skyroam has now discovered evidence that Mr. Wang (1) acquired Plaintiffs' trade secrets by improper means when he copied them onto a USB drive without permission from anyone at Plaintiffs; (2) transferred some or all of the contents of the USB drive copies to his personal home computer; (3) further copied Plaintiffs' trade secrets to his uCloudlink work computer; (4) disclosed Plaintiffs' trade secrets to other uCloudlink employees at various uCloudlink entities—including, but not limited to, the senior executives at Misappropriation Defendants who are listed as co-inventors on the uCloudlink patents that disclose Plaintiffs' trade secrets; (5) and authored patents now assigned to uCloudlink Shenzhen, founded upon Plaintiffs' trade secrets and confidential and proprietary information—all of which have resulted in the manufacture, offer for sale, and sale of products that embody Plaintiffs' trade secrets in the United States.

282. Misappropriation Defendants subsequently used this information in connection with its business activities, in a manner adverse to Plaintiffs' business interests. Such use was and is without Plaintiffs' express or implied consent.

283. uCloudlink Shenzhen's act of listing senior executives of the uCloudlink Group, including but not limited to its CEO, on patent applications that contain Plaintiffs' misappropriated

trade secrets is evidence that the uCloudlink Group knew or had reason to know that its employee, Mr. Wang, improperly obtained Plaintiffs' trade secrets. It is further evidence that the uCloudlink Group knew or should have known that any use of those trade secrets was unauthorized and such use would result in the Misappropriation Defendants competing with and misappropriating Plaintiffs' trade secrets.

284. uCloudlink Hong Kong, uCloudlink Shenzhen, and/or uCloudlink New should be held responsible for the acts of Mr. Wang under the theory of *respondeat superior*.

285. In particular, upon information and belief, Mr. Wang was acting within the scope of his eventual employment by uCloudlink entities at the time he misappropriated Skyroam's trade secrets.

286. Upon information and belief, Mr. Wang was acting in furtherance of uCloudlink's business at the time he misappropriated Skyroam's trade secrets.

287. Upon information and belief, Mr. Wang accomplished an objective for which he was employed relating to developing uCloudlink's cloud-SIM business at the time he misappropriated Skyroam's trade secrets.

288. uCloudlink Hong Kong, uCloudlink Shenzhen, and/or uCloudlink New should be held responsible for the acts of Mr. Wang because at least those three corporate entities and Mr. Wang were engaged in a civil conspiracy.

289. In particular, upon information and belief, the acts of Defendants and Mr. Wang were by two or more persons. These acts were in further of an object to be accomplished in the form of developing uCloudlink's cloud-SIM business. Upon information and belief, Mr. Wang and the Defendants had a meeting of the minds as to the course of action in the form of Mr. Wang obtaining Skyroam confidential information before returning to uCloudlink. Upon information

and belief, Mr. Wang committed one or more unlawful overt acts in taking Skyroam's confidential information.

290. Damages were at least one proximate result of Mr. Wang's acts in taking Skyroam's confidential information.

291. As a result, in violation of Plaintiffs' rights, Misappropriation Defendants misappropriated, and continue to use, Plaintiffs' trade secret information in the improper and unlawful manner described above. Misappropriation Defendants' misappropriation of Plaintiffs' confidential, proprietary, and trade secret information was intentional, knowing, willful, malicious, fraudulent, and oppressive. Misappropriation Defendants have further attempted to and continue to attempt to conceal their misappropriation.

292. Misappropriation Defendants' possession, disclosure, and use of Plaintiffs' trade secrets in the back end systems and the same products accused of patent infringement in the instant litigation is the quintessential example of behavior that rises to the level of "willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant, or—indeed—characteristic of a pirate."

293. As the direct and proximate result of Misappropriation Defendants' conduct in the United States, Plaintiffs have suffered and, if Misappropriation Defendants' conduct is not stopped, will continue to suffer, severe competitive harm, irreparable injury, and significant damages, in an amount to be proven at trial. Because Plaintiffs' remedy at law is inadequate, Plaintiffs seek, in addition to damages, injunctive relief to recover and protect their confidential, proprietary, and trade secret information and to protect other legitimate business interests. Plaintiffs' business operates in a highly competitive market and will continue suffering irreparable harm absent injunctive relief.

294. Plaintiffs have been damaged by all of the foregoing and are entitled to an award of exemplary damages and attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray that this Court:

A. Enter judgment that Defendants have infringed the '689 patent;

B. Enter an order preliminarily and permanently enjoining Defendants, their officers, agents, servants, employees, attorneys, and all persons acting in concert or participation with them, from infringing the '689 Patent;

C. Award Plaintiffs damages resulting from Defendants' patent infringement pursuant to 35 U.S.C. § 284, including for lost profits;

D. Enjoin Defendants from using or otherwise disclosing Plaintiffs' confidential, proprietary, and trade secret information, including by selling products that embody, use, or otherwise rely on such information;

E. Enjoin any destruction, deletion, transfer, copy, download, or other form of reproduction or deletion of any of Plaintiffs' confidential, proprietary, and/or trade secret information in Defendants' possession, custody, or control, unless it is done under the supervision of Plaintiffs' third party forensic investigator;

F. Account for any and all of Plaintiffs' confidential, proprietary, and/or trade secret information currently or previously in Defendants' possession, custody, or control and produce for immediate inspection and imaging all computers and other electronic devices belonging to or under control of, accessible to, or operated by Defendants, including but not limited to Mr. Wang's uCloudlink-issued work computer;

G. Award Plaintiffs damages adequate to compensate for Defendants' misappropriation of Plaintiffs' trade secrets including, but not limited to, actual damages suffered

as a result of the misappropriation, including reasonable royalties and any unjust enrichment as a result of the misappropriations;

H. Find this to be an exceptional case and award Plaintiffs their attorneys' fees and costs, pursuant to 35 U.S.C. § 285;

I. Award Plaintiffs their prejudgment interest and post judgment interest on its damages, attorneys' fees and cost;

J. Award punitive damages to Plaintiffs owing to the willful, wanton, and malicious nature of Defendants' acts;

K. Award Plaintiffs the ownership of all Defendants' patents and patent applications that have been or are obtained using Plaintiffs' confidential, proprietary, and/or trade secret information; and

L. Award Plaintiffs such other and further relief as this Court deems just and proper, including but not limited to an accounting for pre-judgment infringements made but not otherwise awarded to Plaintiffs.

JURY DEMAND

Plaintiffs hereby demand a trial by jury on all issues triable to a jury in this case.

Dated: January 6, 2020

Respectfully Submitted,

By: */s/ Melissa Smith*

Melissa Smith (Texas Bar No. 24001351)
Gillam & Smith LLP
303 South Washington Avenue
Marshall, Texas 75670
Telephone: (903) 934-8450
Facsimile: (903) 934-9257
melissa@gillamsmithlaw.com

Benjamin E. Weed (*pro hac vice* forthcoming)

Gina A. Johnson (*pro hac vice* forthcoming)
Farris S. Matariyeh (*pro hac vice* forthcoming)
benjamin.weed@klates.com
gina.johnson@klgates.com
farris.matariyeh@klgates.com
K&L GATES LLP
70 W. Madison St. Suite 3100
Chicago, IL 60602
Telephone: +1 312 372 1121
Facsimile: +1 312 827 8000

Jeffrey C. Johnson (*pro hac vice* forthcoming)
jeff.johnson@klgates.com
K&L GATES LLP
925 Fourth Avenue, Suite 2900
Seattle, WA 98104
Telephone: +1 206 3708338
Facsimile: +1 206 623 7022

Peter E. Soskin (*pro hac vice* forthcoming)
peter.soskin@klgates.com
K&L GATES LLP
Four Embarcadero Center, Suite 1200
San Francisco, CA 94111
Telephone: +1 415 882 8200
Facsimile: +1 415 882 8220

Attorneys for Plaintiffs
SIMO Holdings Inc., Skyroam, Inc., and Shenzhen Skyroam Technology Co., Ltd.